Release Notes for the Catalyst 4900 Series Switch, Cisco IOS Release 12.2(40)SG

Current Release
12.2(40)SG—November 13, 2007

Previous Releases
12.2(37)SG1, 12..2(37)SG, 12.2(31)SGA5, 12.2(31)SGA4, 12.2(31)SGA3, 12.2(31)SGA2, 12.2(31)SGA1, 12.2(31)SGA, 12.2(31)SG3, 12.2(31)SG2, 12.2(31)SG1, 12.2(31)SG, 112.2(25)SG4, 2.2(25)SG3, 12.2(25)SG2, 12.2(25)SG1, 12.2(25)SG, 12.2(25)EWA13, 12.2(25EWA12, 12.2(25)EWA11, 12.2(25)EWA10, 12.2(25)EWA9, 12.2(25)EWA8, 12.2(25)EWA7, 12.2(25)EWA6, 12.2(25)EWA5, 12.2(25)EWA4, 12.2(25)EWA3, 12.2(25)EWA2, 12.2(25)EWA1, 12.2(25)EW, 12.2(20)EWA4, 12.2(20)EWA3, 12.2(20)EWA2, 12.2(20)EWA1, 12.2(20)EWA

These release notes describe the features, modifications, and caveats for the Cisco IOS software on the Catalyst 4900 series switch. The most current software release is Cisco IOS Release 12.2(40)SG.

The most current software release is Cisco IOS Release 12.2(40)SG. The most current release notes for this release is available on Cisco.com at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_note09186a008062ff34.html

Note Although their *Release Notes* are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst M4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html

Contents

This publication consists of these sections:

- Cisco IOS Software Packaging for the Cisco Catalyst 4900 Series, page 2
- Catalyst 4900 Series Switch Cisco IOS Release Strategy, page 4
- System Requirements, page 5
- New and Changed Information, page 13

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© <2005-2008> Cisco Systems, Inc. All rights reserved.

- Upgrading the System Software, page 18
- Limitations and Restrictions, page 31
- Caveats, page 36
- Troubleshooting, page 128
- Related Documentation, page 130
- Notices, page 132
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 134

Cisco IOS Software Packaging for the Cisco Catalyst 4900 Series

A new Cisco IOS Software package for Cisco Catalyst 4900 Series switches was introduced in Cisco IOS Software Release 12.2(25)SG. It is a new foundation for features and functionality and provides consistency across all Cisco Catalyst switches. The new Cisco IOS Software release train is designated as 12.2SG.

Prior Cisco Catalyst 4900 Series Cisco IOS Software images for the Cisco Catalyst 4900 Series Switches, formerly known as Basic Layer 3 and Enhanced Layer 3, now map to IP Base and Enterprise Services, respectively. Border Gateway Protocol (BGP) is now included in the Enterprise Services image. All currently shipping Cisco Catalyst 4900 software features based on Cisco IOS Software are supported in the IP Base image of Release 12.2(40)SG with a few exceptions.

The IP Base image does not support enhanced routing features such as Nonstop Forwarding/Stateful Switchover (NSF/SSO), BGP, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Internetwork Packet Exchange (IPX), AppleTalk, Virtual Routing Forwarding (VRF-lite), GLBP, and policy-based routing (PBR). The IP Base image supports EIGRP-Stub for limited routing on Cisco Catalyst 4900 Series Switches.

The Enterprise Services image supports all Cisco Catalyst 4900 Series software features based on Cisco IOS Software, including enhanced routing. BGP capability is included in the Enterprises Services package.

Orderable Product Numbers:

- S49IPB-12240SG—Cisco IOS software for the Catalyst 4900 Series (IP Base image) (cat4500-ipbase-mz)
- S49IPBK9-12240SG—Cisco IOS software for the Catalyst 4900 Series (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S49ES-12240SG—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image with BGP support) (cat4500-entservices-mz)
- S49ESK9-12240SG—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image with 3DES and BGP) (cat4500-entservicesk9-mz)
- S49IPB-12237SG—Cisco IOS software for the Catalyst 4900 Series (IP Base image) (cat4500-ipbase-mz)
- S49IPBK9-12237SG—Cisco IOS software for the Catalyst 4900 Series (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S49ES-12237SG—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image) (cat4500-entservices-mz)

- S49ESK9-12237SG—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image with 3DES) (cat4500-entservicesk9-mz)
- S49IPB-12231SGA—Cisco IOS software for the Catalyst 4900 Series (IP Base image) (cat4500-ipbase-mz)
- S49IPBK9-12231SGA—Cisco IOS software for the Catalyst 4900 Series (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S49ES-12231SGA—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image) (cat4500-entservices-mz)
- S49ESK9-12231SGA—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image with 3DES) (cat4500-entservicesk9-mz)

Note We recommend that you load 12.2(31)SGA4.

- S49IPB-12231SG—Cisco IOS software for the Catalyst 4900 Series (IP Base image) (cat4500-ipbase-mz)
- S49IPBK9-12231SG—Cisco IOS software for the Catalyst 4900 Series (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S49ES-12231SG—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image) (cat4500-entservices-mz)
- S49ESK9-12231SG—Cisco IOS software for the Catalyst 4900 Series (Enterprise Services image with 3DES) (cat4500-entservicesk9-mz)
- S49IPB-12225SG—Cisco IOS software for the Catalyst 4900 Series Switch (IP Base image) (cat4500-ipbase-mz)
- S49IPBK9-12225SG—Cisco IOS software for the Catalyst 4900 Series Switch (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S49ES-12225SG—Cisco IOS software for the Catalyst 4900 Series Switch (Enterprise Services image with BGP support) (cat4500-entservices-mz)
- S49ESK9-12225SG—Cisco IOS software for the Catalyst 4900 Series Switch (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S4KL3-12225EWA—Cisco IOS software for the Catalyst 4900 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX Software Routing, Release 12.2(25)EWA (cat4000-i9s-mz.122-25.EWA)
- S4KL3E-12225EWA—Cisco IOS software for the Catalyst 4900 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(25)EWA (cat4000-i5s-mz.122-25.EWA)
- S4KL3K9-12225EWA—Cisco IOS software for the Catalyst 4900 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(25)EWA (cat4000-i9k9s-mz.122-25.EWA)
- S4KL3EK9-12225EWA—Cisco IOS software for the Catalyst 4900 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, IGRP, and EIGRP), Release 12.2(25)EWA (cat4000-i5k9s-mz.122-25.EWA)
- S4KL3-12220EWA—Cisco IOS software for the Catalyst 4900 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX Software Routing, Release 12.2(20)EWA (cat4000-i9s-mz.122-20.EWA)

- S4KL3E-12220EWA—Cisco IOS software for the Catalyst 4900 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(20)EWA (cat4000-i5s-mz.122-20.EWA)
- S4KL3K9-12220EWA—Cisco IOS software for the Catalyst 4900 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(20)EWA (cat4000-i9k9s-mz.122-20.EWA)
- S4KL3EK9-12220EWA—Cisco IOS software for the Catalyst 4900 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, IGRP, and EIGRP), Release 12.2(20)EWA (cat4000-i5k9s-mz.122-20.EWA)
- S4KL3-12220EW—Cisco IOS software for the Catalyst 4900 series switch, basic Layer 3 and voice software image (RIPv1, RIPv2, Static Routes, AppleTalk, and IPX), Release Software Routing, Release 12.2(20)EW (cat4000-i9s-mz.122-20.EW)
- S4KL3E-12220EW—Cisco IOS software for the Catalyst 4900 series switch, enhanced Layer 3 and voice software image including OSPF, IS-IS, and EIGRP, Release 12.2(20)EW (cat4000-i5s-mz.122-20.EW)
- S4KL3K91-12220EW—Cisco IOS software for the Catalyst 4900 series switch, with 3DES strong encryption, basic Layer 3 and voice software image (SSHv1, SSHv2, RIPv1, RIPv2, static routes, AppleTalk, and IPX), Release 12.2(20)EW (cat4000-i9k91s-mz.122-20.EW)
- S4KL3EK91-12220EW—Cisco IOS software for the Catalyst 4900 series switch, with 3DES strong encryption, enhanced Layer 3 and voice software image including (OSPF, IS-IS, and EIGRP), Release 12.2(20)EW (cat4000-i5k91s-mz.122-20.EW)

Catalyst 4900 Series Switch Cisco IOS Release Strategy

Customers with Catalyst 4900 series switches who need the latest hardware support and software features should migrate to Cisco IOS Release 12.2(40)SG.

For more information on the Catalyst 4900 series switches, visit the following URL: www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm

Cisco IOS Software Migration

Figure 1 displays the Cisco IOS Software Release 12.2(40)SG plan relative to the 12.2S release train and identifies the recommended migration path. Note that 12.2(40)SG will not be the base release for a new maintenance train. Moving forward, the Cisco Catalyst 4900 platform has two active maintenance trains: 12.2(25)EWA and 12.2(31)SGA.

Figure 1 Software Release Strategy for the Catalyst 4900 Series Switch

Summary of Migration Plan

- Customers requiring the latest Cisco Catalyst 4900 Series hardware and software features should migrate to Cisco IOS Software Release 12.2(40)SG.
- Cisco IOS Software Release 12.2(31)SGA will continue offering maintenance releases. The latest release from the 12.2(31)SGA maintenance train is 12.2(31)SGA4.
- Cisco IOS Software Release 12.2(25)EWA will continue offering maintenance releases. The latest release from the 12.2(25)EWA maintenance train is 12.2(25)EWA10.

Support

Support for Cisco IOS Software Release 12.2(40)SG follows the standard Cisco Systems® support policy, available at http://www.cisco.com/en/US/products/products_end-of-life_policy.html

For more information about the Cisco Catalyst 4900 series switch, visit http://www.cisco.com/en/US/products/ps6021/index.html

System Requirements

This section describes the system requirements:

- Memory Requirements, page 6
- Supported Hardware, page 6
- Supported Features, page 7
- Unsupported Features, page 12

Memory Requirements

These are the minimum required memory configurations for Cisco IOS software on the Catalyst 4900 series switch:

- 256-MB SDRAM DIMM
- 64-MB Flash SIMM

Supported Hardware

The following tables lists the hardware supported on the Catalyst 4900 series switch.

Table 1 Supported Hardware

Product Number (append with "=" for spares)	**Product Description**	**Software Release**	
		Minimum	**Recommended**
Small Form-Factor Pluggable Modules			
GLC-BX-D	1000BASE-BX10-D small form-factor pluggable module	12.2(20)EWA	12.2(31)SGA4
GLC-BX-U	1000BASE-BX10-U small form-factor pluggable module	12.2(20)EWA	12.2(31)SGA4
GLC-SX-MM	1000BASE-SX small form-factor pluggable module	12.2(20)EWA	12.2(31)SGA4
GLC-LH-SM	1000BASE-LX/LH small form-factor pluggable module	12.2(20)EWA	12.2(31)SGA4
GLC-ZX-SM	1000BASE-ZX small form-factor pluggable module	12.2(20)EWA	12.2(31)SGA4
GLC-T	1000BASE-T small form-factor pluggable module	12.2(20)EWA	12.2(31)SGA4
CWDM-SFP-xxxx	CWDM small form-factor pluggable module (See Table 2 on page 6 for a list of supported wavelengths.)	12.2(20)EWA	12.2(31)SGA4
10 Gigabit Ethernet X2 Pluggable Modules			
X2-10GB-LR	10GBASE-LR single-mode X2 module	12.2(25)EWA	12.2(31)SGA4
X2-10GB-SR	10GBASE-SR single-mode X2 module	12.2(25)EWA	12.2(31)SGA4
X2-10GB-CX4	10GBASE-CX4 single-mode X2 module	12.2(25)EWA	12.2(31)SGA4
X2-10GB-LX4	10GBASE-LX4 single-mode X2 module	12.2(25)EWA	12.2(31)SGA4
X2-10GB-LRM	10GBASE-LRM single-mode X2 module	12.2(31)SGA	12.2(31)SGA3
X2-10GB-ER	10GBASE-ER single-mode X2 module	12.2(25)EWA	12.2(31)SGA4

Table 2 briefly describes the supported wavelengths in the Catalyst 4900 series switches.

Table 2 CWDM SFP Supported Wavelengths

Product Number (append with "=" for spares)	**Product Description**	**Software Release**	
		Minimum	**Recommended**
CWDM-SFP -1470	Longwave 1470 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4
CWDM- SFP -1490	Longwave 1490 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4
CWDM-SFP -1510	Longwave 1510 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4

Table 2 CWDM SFP Supported Wavelengths

Product Number (append with "=" for spares)	**Product Description**	**Software Release**	
		Minimum	**Recommended**
CWDM-SFP -1530	Longwave 1530 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4
CWDM-SFP -1550	Longwave 1550 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4
CWDM-SFP -1570	Longwave 1570 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4
CWDM-SFP -1590	Longwave 1590 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4
CWDM-SFP -1610	Longwave 1610 nm laser single-mode	12.2(20)EWA	12.2(31)SGA4

Table 3 briefly describes the Catalyst 4900 product set.

Table 3 WS-4948 and WS-4948-10GE

Product Number (append with "=" for spares)	**Product Description**	**Software Release**	
		Minimum	**Recommended**
WS-X4948	48-port 10/100/1000 Catalyst 4948 switch, optional software image, optional power supplies, fan tray	12.2(20)EWA	12.2(31)SGA4
WS-X4948-S	48-port 10/100/1000 Catalyst 4948 switch, SMI, one AC power supply, fan tray	12.2(20)EWA	12.2(31)SGA4
WS-X4948-E	48-port 10/100/1000 Catalyst 4948 switch, EMI, one AC power supply, fan tray	12.2(20)EWA	12.2(31)SGA4
WS-X4948-10GE	48-port 10/100/1000 2-10GE Catalyst 4948 switch, optional software image, optional power supplies, fan tray	12.2(25)EWA	12.2(31)SGA4
WS-X4948-10GE-S	48-port 10/100/1000 2-10GE Catalyst 4948 switch, SMI, one AC power supply, fan tray	12.2(25)EWA	12.2(31)SGA4
WS-X4948-10GE-E	48-port 10/100/1000 2-10GE Catalyst 4948 switch, EMI, one AC power supply, fan tray	12.2(25)EWA	12.2(31)SGA4

Supported Features

Table 4 lists the Cisco IOS software features for the Catalyst 4900 series switch.

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900 Series Switch

Layer 2 Switching Features
Storm control
Multicast storm control
IP Source Guard
IP Source Guard for Statis Hosts
PVRST+
Layer 2 protocol tunneling
Layer 2 transparent bridging[1]

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900 Series Switch (continued)

Layer 2 MAC[2] learning, aging, and switching by software
Unicast MAC address filtering
VMPS[3] Client
Layer 2 hardware forwarding up to 102 Mpps
Layer 2 switch ports and VLAN trunks
Spanning-Tree Protocol (IEEE 802.1D) per VLAN
802.1s and 802.1w
Layer 2 traceroute
Unidirectional Ethernet port
Per-VLAN spanning tree (PVST) and PVST+
Spanning-tree root guard
Spanning-tree Loop guard and PortFast BPDU Filtering
Support for 9216 byte frames
Port security on PVLANs
Private VLANs
Private VLAN DHCP snooping
Community PVLANs
Private VLAN Promiscuous Trunk
ISL
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
Support for 4096 VLANs per switch
Unidirectional link detection (UDLD) and aggressive UDLD
Layer 3 Routing, Switching, and Forwarding
802.1Q Tunneling (Q in Q)[4]
QinQ and Protocol Tunneling
Pragmatic General Multicast
Auto RP Listener
IP and IP multicast routing and switching between Ethernet ports
Static IP routing
Classless routing[5]
PBR[6]
Dynamic Buffer Limiting
Selective Dynamic Buffer Limiting
QoS-based forwarding based on IP precedence
Trusted boundary

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900 Series Switch (continued)

Auto QoS
Match CoS for non-IPV4 traffic
CoS Mutation
CEF[7] load balancing
Hardware-based IP CEF routing at 102 Mpps
Up to 128,000 IP routes
Up to 32,000 IP host entries (Layer 3 adjacencies)
Up to 16,000 IP multicast route entries
Up to 55,000 unicast entries
Multicast flooding suppression for STP changes
Software routing of IPX, AppleTalk, and IPv6
IGMPv1, IGMPv2, and IGMPv3 (Full Support)
VRF-lite
Route Leaking[8]
IP Unnumbered
SVI Autostate Exclude
Supported Protocols
IS-IS[9]
DTP[10]
RIP[11] and RIP II
EIGRP[12]
EIGRP stub
OSPF[13]
BGP4[14]
BGP route-map Continue
BGP Neighbor Policy
MBGP[15]
MSDP[16]
ICMP[17] Router Discovery Protocol
PIM[18]—sparse and dense mode
Static routes
Classless interdomain routing (CIDR)
DVMRP[19]
SSM
NTP[20]
WCCPv2 Layer 2 Redirection
VRRP[21]

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900 Series Switch (continued)

SCP[22]
GLBP[23]
EtherChannel Features
Cisco EtherChannel technology - 10/100/1000 Mbps, 10 Gbps
Load balancing for routed traffic, based on source and destination IP addresses
Load sharing for bridged traffic based on MAC addresses
ISL on all EtherChannels
IEEE 802.1Q on all EtherChannels
Bundling of up to eight Ethernet ports
Up to 50 active Ethernet port channels
Trunk Port Security over EtherChannel
Additional Protocols and Features
SPAN CPU port mirroring
SPAN packet-type filtering
SPAN destination in-packets option
SPAN ACL filtering
RSPAN[24]
Enhanced VLAN statistics
Secondary addressing
Bootstrap protocol (BOOTP)
Authentication, authorization, and accounting using TACACS+ and RADIUS protocol
Cisco Discovery Protocol (CDP)
Sticky port security
Trunk port security
Voice VLAN Sticky Port Security
Cisco Group Management Protocol (CGMP) server support
HSRP[25] over Ethernet, EtherChannels - 10/100/1000Mbps, 10 Gbps
IGMP[26] snooping version1, version 2, and version 3 (Full Support)
IGMP filtering
Port Aggregation Protocol (PagP)
802.3ad LACP
SSH version 1 and version 2[27]
show interface capabilities command
IfIndex persistence
UDLR[28]
Enhanced SNMP MIB support
SNMP[29] version 1, version 2, and version 3

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900 Series Switch (continued)

SNMP version 3 (with encryption)
DHCP server and relay-agent
DHCP snooping
DHCP client autoconfiguration
DHCP Option 82 Pass Through
802.1X port-based authentication
802.1X with port security
802.1X accounting
802.1X with voice VLAN ID[30]
802.1X private VLAN assignment
802.1X private guest VLAN
802.1X RADIUS-supplied session timeout
802.1X authentication failure VLAN
802.1X MAC Authentication Bypass
802.1X Inaccessible Authentication Bypass
802.1X Unidirectional Controlled Port
Control Plane Policing
Port flood blocking
Router standard and extended ACLs [31]on all ports with no performance penalty
Extended IPX Access Control Lists
VLAN Access Control Lists
PACL[32]
Local Proxy ARP
Dynamic ARP Inspection on PVLANs
Dynamic ARP Inspection
Per-port QoS[33] rate-limiting and shaping
Per-port Per-VLAN QoS
Power redundancy
Non-stop Forwarding Awareness
Non-stop Forwarding Awareness for EIGRP-stub in IP base for all supervisor engines
WCCP[34]v2 Layer 2 Redirection
MAC Address Notification
SmartPort macros
802.1s standards compliance
IS-IS MIB
OSPF Fast Convergence
Time Domain Reflectometry

Table 4 Cisco IOS Software Feature Set for the Catalyst 4900 Series Switch (continued)

CNA[35]
EEM[36]

1. Hardware-based transparent bridging within a VLAN
2. MAC = Media Access Control
3. VMPS = VLAN Management Policy Server
4. Requires the Catalyst 4900 series switch Supervisor Engine V
5. The **ip classless** command is not supported as classless routing is enabled by default.
6. PBR = policy-based routing
7. CEF = Cisco Express Forwarding
8. Route Leaking from a global routing table into a VRF and Route Leaking from a VRF into a global routing table
9. IS-IS = Intermediate System to Intermediate System
10. DTP = Dynamic Trunking Protocol
11. RIP = Routing Information Protocol
12. EIGRP = Enhanced Interior Gateway Routing Protocol
13. OSPF = Open Shortest Path First
14. BGP4 = Border Gateway Protocol 4
15. MBGP = Multicast Border Gateway Protocol
16. MSDP = Multicast Source Discovery Protocol
17. ICMP = Internet Control Message Protocol
18. PIM = Protocol Independent Multicast
19. DVMRP = Distance Vector Multicast Routing Protocol
20. NTP = Network Time Protocol
21. VRRP = Virtual Router Redundancy Protocol
22. SCP = Secure Copy Protocol
23. GLBP = Gateway Load Balancing Protocol
24. RSPAN = Remote SPAN
25. HSRP = Hot Standby Router Protocol
26. IGMP = Internet Group Management Protocol
27. SSH = Secure Shell Protocol
28. UDLR = Unidirectional Link Routing
29. SNMP = Simple Network Management Protocol
30. PoE is not supported on the Catalyst 4900 series switch.
31. ACLs = Access Control Lists
32. PACL = Port Access Control List
33. QoS = Quality of Service
34. WCCP = Web Content Communication Protocol
35. CNA = Cisco Network Assistant; Minimum CNA release that supports Releases 12.2(25)EW is 1.0(2). Minimum CNA release that supports Release 12.2(20)EWA is 1.0(1).
36. EEM = Embedded Event anager

Unsupported Features

These features are not supported in Cisco IOS Release 12.2(40)SG for the 4900 series switches:

- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list

  - DECnet access list
  - Protocol type-code access list
- Cisco IOS software IPX ACLs:
  - <1200-1299> IPX summary address access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- IGRP (use EIGRP instead)
- **isis network point-to-point** command
- Kerberos support for access control
- Lock and key
- NAT-PT for IPv6
- NetFlow
- PBR with Multiple Tracking Options
- QoS for IPv6 (QoS for IPv6 traffic)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- Two-way community VLANs in private VLANs
- Automatic shutdown due to overtemperature

  The IOS software sends system messages when the internal temperature (as read from sensors on the supervisor engine) reaches 75 and 95 degrees Celsius. A power supply may shut down when the ambient temperature exceeds 55 degrees C.

New and Changed Information

These sections describe the new and changed information for the Catalyst 4900 series switch running Cisco IOS software:

- New Hardware Features in Release 12.2(40)SG, page 14
- New Software Features in Release 12.2(40)SG, page 14
- New Hardware Features in Release 12.2(37)SG, page 14
- New Software Features in Release 12.2(37)SG, page 14
- New Hardware Features in Release 12.2(31)SGA, page 15
- New Software Features in Release 12.2(31)SGA, page 15
- New Hardware Features in Release 12.2(31)SG, page 16
- New Software Features in Release 12.2(31)SG, page 16

- New Hardware Features in Release 12.2(25)SG, page 16
- New Software Features in Release 12.2(25)SG, page 16
- New Hardware Features in Release 12.2(25)EWA, page 17
- New Software Features in Release 12.2(25)EWA, page 17
- New Hardware Features in Release 12.2(25)EW, page 18
- New Software Features in Release 12.2(25)EW, page 18
- New Hardware Features in Release 12.2(20)EWA, page 18
- New Software Features in Release 12.2(20)EWA, page 18

New Hardware Features in Release 12.2(40)SG

Release 12.2(40)SG provides the following new hardware for the Catalyst 4900 series switch:

- None

New Software Features in Release 12.2(40)SG

Release 12.2(40)SG provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Embedded Event Manager (Refer to the Cisco IOS Release 12.4 documentation)
- Gateway Load Balancing Protocol (Refer to the Cisco IOS Release 12.4 documentation)

New Hardware Features in Release 12.2(37)SG

Release 12.2(37)SG provides the following new hardware for the Catalyst 4900 series switch:

- None

New Software Features in Release 12.2(37)SG

Release 12.2(37)SG provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Selective Dynamic Buffer Limiting (“Configuring QoS” chapter)
- SVI Autostate Exclude (“Configuring Layer 3 Interface” chapter)

- IP Source Guard for Statis Hosts (“Configuring DHCP Snooping, IP Source Guard, and IPSG for Statis Hosts” chapter)
- BGP route-map Continue Support for Outbound Policy

  For details, locate the feature entry in the Feature Information Table located toward the end of the "Connecting to a Service Provider Using External BGP" module:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tbgp_c/t_brbext.htm
- Auto RP Listerner (Refer to the Cisco IOS Release 12.4 documentation)

New Hardware Features in Release 12.2(31)SGA

Cisco IOS Release 12.2(31)SGA is the first IOS release supporting the Cisco ME 4900 Series Ethernet Switch.

Following hardware was supported:

- X2-10GB-LRM

New Software Features in Release 12.2(31)SGA

Release 12.2(31)SGA provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Trunk Port Security over EtherChannel (“Configuring Port Security and Configuring EtherChannel” chapters)
- Match CoS for Non-IPv4 Traffic (“Configuring QoS” chapter)
- CoS Mutation (“Configuring QoS” chapter)
- QinQ Tunneling and Protocol Tunneling (“Configuring 802.1Q and Layer 2 Protocol Tunneling” chapter)
- IP Unnumbered (“Configuring IP Unnunmbered Support” chapter)

New Hardware Features in Release 12.2(31)SG

There are no new hardware features in Cisco IOS Release 12.2(31)SG.

New Software Features in Release 12.2(31)SG

Release 12.2(31)SG provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Control Plane Policing (“Configuring Control Plane Policing” chapter)
- WCCPv2 Layer 2 Redirection (“Configuring WCCPv2 Services” chapter)
- MAC Authentication Bypass (“Configuring 802.1X Port-Based Authentication” chapter)
- 802.1X Inaccessible Authentication Bypass (“Configuring 802.1X Port-Based Authentication” chapter)
- 802.1X Unidirectional Controlled Port (“Configuring 802.1X Port-Based Authentication” chapter)
- Private VLAN Promiscuous Trunk (“Configuring Private VLANs” chapter)
- MAC Address Notification (“Administering the Switch” chapter)
- Voice VLAN Sticky Port Security (“Configuring Port Security” chapter)
- Virtual Router Redundancy Protocol (VRRP) (Refer to the Cisco IOS Release 12.3 documentation)
- Secure Copy Protocol (SCP) (Refer to the Cisco IOS Release 12.3 documentation)

New Hardware Features in Release 12.2(25)SG

There are no new hardware features in Cisco IOS Release 12.2(25)SG.

New Software Features in Release 12.2(25)SG

Release 12.2(25)SG provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- 802.1X Authentication Failure VLAN (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- HTTPS (Refer to the Cisco IOS Release 12.3 documentation)
- IS-IS MIB (Refer to the Cisco IOS Release 12.3 documentation
- OSPF Fast Convergence (Refer to the Cisco IOS Release 12.3 documentation)

- Time Domain Reflectometry (“Checking Port Status and Connectivity” chapter)

New Hardware Features in Release 12.2(25)EWA

Release 12.2(25)EWA provides the following new hardware for the Catalyst 4900 series switch:

- WS-X4948-10GE—Catalyst 4948 48-Port 10/100/1000 + 2 10GE in a 1 RU with dual, redundant AC/DC power

Caution If you plan to insert X2 transceivers in the Cisco Catalyst 4948-10GE, you should ensure that the Catalyst 4900 series switch and the X2 back interfaces are properly oriented during the OIR (Online insertion and removal) of the transceivers. The top transceiver (port tengig1/49) should be inserted with heatsink facing up. The bottom transceiver (port tengig1/50) should be plugged in with heatsink facing down, CLEI (Common Language Equipment Identifiers) label facing up. When inserted correctly, the TX/RX of the bottom transceiver would look reversed. For more details refer to the *Catalyst 4948-10GE Switch Installation Guide*, at the URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/hw_doc/4948_10/05modcfg.htm#wp1038597

New Software Features in Release 12.2(25)EWA

Release 12.2(25)EWA provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Per-Port Per-VLAN QoS (“Configuring QoS and Per-Port Per-VLAN QoS” chapter)
- Trunk-Port Security (“Configuring Port Security and Trunk Port Security” chapter)
- 802.1X Private VLAN Assignment (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- 802.1X Private Guest VLAN (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- 802.1X Radius-Supplied Session Timeout (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- DHCP Option 82 Pass Through (“Configuring DHCP Snooping and IP Source Guard” chapter)

New Hardware Features in Release 12.2(25)EW

There are no new hardware features in Release 12.2(25)EW.

New Software Features in Release 12.2(25)EW

There are no new software features in Cisco IOS Release 12.2(25)EW

New Hardware Features in Release 12.2(20)EWA

There are no new hardware features in Cisco IOS Release 12.2(20)EWA.

New Software Features in Release 12.2(20)EWA

Release 12.2(20)EWA provides the following Cisco IOS software features for the Catalyst 4900 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- 802.1X with Voice VLAN ID ("Understanding and Configuring 802.1X Port-Based Authentication" chapter)
- Forced 10/100 Auto Negotiation ("Configuring Interfaces" chapter)

Upgrading the System Software

In most cases, upgrading the switch to a newer release of Cisco IOS software does not require a ROMMON upgrade. However, if you are running an early release of Cisco IOS software and plan to upgrade, the following tables list the recommended ROMMON release.

Caution Most supervisor engines have the required ROMMON release. However, due to caveat CSCed25996, we recommend that you upgrade your ROMMON to the recommended release.

Table 5 Catalyst 4900 Series Switches, Recommended ROMMON Release, and Promupgrade Programs

Switching Module	Minimum ROMMON Release	Recommended ROMMON Release	Promupgrade Program
WS-X4948	12.2(20r)EW	12.2(31r)SGA1	cat4500-ios-promupgrade-122_31r_SGA
WS-X4948-10GE	12.2(25r)EWA	12.2(31r)SGA1	cat4500-ios-promupgrade-122_31r_SGA

The following sections describe how to upgrade your switch software:

- Upgrading the ROMMON from the Console, page 19

- Upgrading the ROMMON Remotely Using Telnet, page 22
- Upgrading the Cisco IOS Software, page 27

Upgrading the ROMMON from the Console

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Note The examples in this section use the programmable read-only memory (PROM) upgrade version 12.2(25r)EWA and Cisco IOS Release 12.2(25)EWA. For other releases, replace the ROMMON release and Cisco IOS software release with the appropriate releases and filenames.

Follow this procedure to upgrade your supervisor engine ROMMON:

Step 1 Directly connect a serial cable to the console port.

Note This section assumes that the console baud rate is set to 9600 (default). If you want to use a different baud rate, change the configuration register value for your switch.

Step 2 Download the **cat4000-ios-promupgrade-122_25r_EWA** program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch that will be upgraded.

The **cat4000-ios-promupgrade-122_25r_EWA** programs are available on Cisco.com at the same location from which you download Catalyst 4000 system images.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then issue the **squeeze bootflash:** command to reclaim the space.

Step 4 Download the **cat4000-ios-promupgrade-122_25r_EWA** program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image **cat4000-ios-promupgrade-122_25r_EWA** from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-122_25r_EWA]?
Destination filename [cat4000-ios-promupgrade-122_25r_EWA]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-122_25r_EWA...
Loading cat4000-ios-promupgrade-122_25r_EWA from 172.20.58.78 (via
FastEthernet2/1):!!!
```

```
Proceed with reload? [confirm]

2d11h: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command
.
************************************************************
 *                                                          *
 * Welcome to Rom Monitor for WS-C4948-10GE System.         *
 * Copyright (c) 1999-2005 by Cisco Systems, Inc.           *
 * All rights reserved.                                     *
 *                                                          *
 ************************************************************

 Rom Monitor Program Version 12.2(25r)EWA
 Supervisor: WS-C4948-10GE  Chassis: WS-C4948
 Hardware Revisions - Board: 8.3 CPLD Gill: 17

 MAC Address  : 00-0b-fc-ff-3b-ff
 IP Address   : 10.5.43.225
 Netmask      : 255.255.255.0
 Gateway      : 10.5.43.1
 TftpServer   : 10.5.5.5

 ***** The system will autoboot in 5 seconds *****

 Type control-C to prevent autobooting.
 . .
 Autoboot cancelled......... please wait!!!

 Autoboot cancelled......... please wait!!!
rommon 1 > [interrupt]
```

Step 6 Run the PROM upgrade program by entering this command:
boot bootflash:cat4000-ios-promupgrade-122_25r_EWA

Caution No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the output from a successful upgrade, followed by a system reset:

```
rommon 2 > boot bootflash:cat4000-ios-promupgrade-122_25r_EWA


 ************************************************************
 *                                                          *
 * Rom Monitor Upgrade Utility For WS-C4948-10GE System     *
 * This upgrades flash Rom Monitor image to the latest      *
 *                                                          *
 * Copyright (c) 1997-2005 by Cisco Systems, Inc.           *
 * All rights reserved.                                     *
 *                                                          *
 ************************************************************

 Image size = 1024.0 KBytes

 Maximum allowed size = 1048576 KBytes


 Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!
```

```
Beginning erase of 0x100000 bytes at offset 0x3e00000...  Done!

Beginning write of prom  (0x100000 bytes at offset 0x3e00000)...

This could take as little as 30 seconds or up to 2 minutes.
Please DO NOT RESET!

Verifying...

Success! The prom has been upgraded successfully.
System will reset itself and reboot within few seconds....
```

Step 7 Boot the Cisco IOS software image, and enter the **show version** command to verify that ROMMON has been upgraded to 12.2(25r)EWA.

Step 8 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the **cat4000-ios-promupgrade-122_25r_EWA** image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4000-ios-promupgrade-122_25r_EWA
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

Step 9 Use the **show version** command to verify that the ROMMON has been upgraded

```
Switch# show version
Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914

ROM: 12.2(25r)EWA
Pod Revision 0, Force Revision 31, Tie Revision 17

Switch uptime is 1 minute
System returned to ROM by reload
System image file is "bootflash:cat4500-ipbase-mz.122-25.EWA"

cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memory.
Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Configuration register is 0x2

Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 27 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the ROMMON Remotely Using Telnet

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Follow this procedure to upgrade your supervisor engine ROMMON to Release 12.2(25r)EWA. This procedure can be used when console access is not available and when the ROMMON upgrade must be performed remotely.

Note In the following section, use the PROM upgrade version **cat4000-ios-promupgrade-122_25r_EWA**.

Step 1 Establish a Telnet session to the supervisor engine.

Note In the following discussion, we assume that at least one IP address has been assigned to either an SVI or a routed port.

Step 2 Download the **cat4000-ios-promupgrade-122_25r_EWA** program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The **cat4000-ios-promupgrade-122_25r_EWA** programs are available on Cisco.com at the same location from which you download Catalyst 4000 system images.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then issue the **squeeze bootflash:** command to reclaim the space.

Step 4 Download the **cat4000-ios-promupgrade-122_25r_EWA** program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image **cat4000-ios-promupgrade-122_25r_EWA** from the remote host 10.5.5.5 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [10.5.5.5]?
Source filename [cat4000-ios-promupgrade-122_25r_EWA]?
/tftpboot/pjose/cat4000-ios-promupgrade-122_25r_EWA
Destination filename [cat4000-ios-promupgrade-122_25r_EWA]?
Accessing tftp://10.5.5.5//tftpboot/pjose/cat4000-ios-promupgrade-122_25r_EWA...
Loading /tftpboot/pjose/cat4000-ios-promupgrade-122_25r_EWA from 10.5.5.5 (via G
igabitEthernet1/1): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1244496 bytes]

1244496 bytes copied in 9.484 secs (131221 bytes/sec)
Switch#
```

Step 5 Use the **no boot system flash bootflash:***file_name* command to clear all BOOT variable commands in the configuration file. In this example, the BOOT variable was set to boot the image **cat4000-ios-promupgrade-122_25r_EWA** from bootflash:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-ios-promupgrade-122_25r_EWA
Switch(config)# exit
```

```
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#

Use the boot system flash bootflash:file_name command to set the BOOT variable. You will
use two BOOT commands: one to upgrade the ROMMON and a second to load the Cisco IOS
software image after the ROMMON upgrade is complete. Notice the order of the BOOT
variables in the example below. At bootup the first BOOT variable command upgrades the
ROMMON. When the upgrade is complete the supervisor engine will autoboot, and the second
BOOT variable command will load the Cisco IOS software image specified by the second BOOT
command.
```

Note The **config-register** must be set to autoboot.

```
In this example, we assume that the console port baud rate is set to 9600 bps and that the
config-register is set to 0x0102.

Use the config-register command to autoboot using image(s) specified by the BOOT variable.
Configure the BOOT variable to upgrade the ROMMON and then autoboot the IOS image after
the ROMMON upgrade is complete. In this example, we are upgrading the ROMMON to version
12.2(25r)EWA. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco
IOS software Release 12.2(25)EWA.

config-register to 0x0102.

Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-ios-promupgrade-122_25r_EWA
Switch(config)# boot system flash bootflash:cat4500-ipbase-mz.122-25.EWA
Switch(config)# config-register 0x0102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 6 Use the **show bootvar** command to verify the boot string. The BOOT variable in this example will first run the PROM upgrade to upgrade ROMMON. Then, the upgrade software will reload and the supervisor engine will load the Cisco IOS software image.

```
Switch#sh bootvar
BOOT variable =
bootflash:cat4000-ios-promupgrade-122_25r_EWA,1;bootflash:cat4500-ipbase-mz.122-25.EWA
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
```

Step 7 Run the PROM upgrade program by issuing the **reload** command. Issuing this command will terminate your Telnet session.

Caution Verify the boot string in step 6. No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the console port output from a successful ROMMON upgrade followed by a system reset. Your Telnet session will be disconnected during the ROMMON upgrade, so you will not see this output. This step could take 2-3 minutes to complete. You will need to reconnect your Telnet session after 2-3 minutes when the Cisco IOS software image and the interfaces are loaded.

```
Switch# reload
Proceed with reload? [confirm]

00:00:36: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.


************************************************************
*                                                          *
* Welcome to Rom Monitor for WS-C4948-10GE System.         *
* Copyright (c) 1999-2005 by Cisco Systems, Inc.           *
* All rights reserved.                                     *
*                                                          *
************************************************************

Rom Monitor Program Version 12.2(25r)EWA
Supervisor: WS-C4948-10GE  Chassis: WS-C4948
Hardware Revisions - Board: 8.0 CPLD : 17 FPGA : 0

MAC Address  : 00-0b-fc-ff-3b-ff
IP Address   : 10.5.43.225
Netmask      : 255.255.255.0
Gateway      : 10.5.43.1
TftpServer   : 10.5.5.5

***** The system will autoboot in 5 seconds *****

Type control-C to prevent autobooting.
. . . . .
******** The system will autoboot now ********

config-register = 0x102
Autobooting using BOOT variable specified file.....
Current BOOT file is --- bootflash:cat4000-ios-promupgrade-122_25r_EWA




************************************************************
*                                                          *
* Rom Monitor Upgrade Utility For WS-C4948-10GE System     *
* This upgrades flash Rom Monitor image to the latest      *
*                                                          *
* Copyright (c) 1997-2005 by Cisco Systems, Inc.           *
* All rights reserved.                                     *
*                                                          *
************************************************************
Image size = 1024.0 KBytes
Maximum allowed size = 1048576 KBytes

Upgrading your PROM... DO NOT RESET the system
unless instructed or upgrade of PROM will fail !!!
Beginning erase of 0x100000 bytes at offset 0x3e00000...  Done!
Beginning write of prom  (0x100000 bytes at offset 0x3e00000)...
This could take as little as 30 seconds or up to 2 minutes.
Please DO NOT RESET!
Verifying...
Success! The prom has been upgraded successfully.
```

```
 System will reset itself and reboot within few seconds....

****
 (output truncated)
 . . . . .
 ******** The system will autoboot now ********

 config-register = 0x102
 Autobooting using BOOT variable specified file.....
 Current BOOT file is --- bootflash:cat4500-ipbase-mz.122-25.EWA
Rommon reg: 0x00004180
############
(output truncated)
Exiting to ios...
Rommon reg: 0x00000180
##############################
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914


cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memory.
Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.
Uncompressed configuration from 1171 bytes to 2726 bytes

Press RETURN to get started!

Switch>en
Switch#
```

Step 8 Use the **no boot system flash bootflash:***file_name* command to clear the BOOT command used to upgrade the ROMMON.

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-ios-promupgrade-122_25r_EWA
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 9 Use the **show version** command to verify that the ROMMON has been upgraded.

```
Switch# show version
```

```
Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914

ROM: 12.2(25r)EWA
Pod Revision 0, Force Revision 31, Tie Revision 17

Switch uptime is 0 minutes
System returned to ROM by reload
System image file is "bootflash:cat4500-ipbase-mz.122-25.EWA"

cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memory.
Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Configuration register is 0x102

Switch#
```

Step 10 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the **cat4000-ios-promupgrade-122_25r_EWA** image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4000-ios-promupgrade-122_25r_EWA
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

Step 11 Use the **show bootvar** command to verify that the ROMMON upgrade program has been removed from the BOOT variable.

```
Switch# show bootvar
BOOT variable = bootflash:cat4500-ipbase-mz.122-25.EWA,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 27 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

Caution To avoid actions that might make your system unable to boot, please read this entire section before starting the upgrade.

Before you proceed, observe the following rules for hostname:

- Do not expect case to be preserved

  Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, Choosing a Name for Your Computer.
- Must start with a letter and end with a letter or digit.
- Interior characters can only be letters, digits, and hyphens; periods and underscores not allowed.
- Names must be 63 characters or fewer; hostname of fewer than 10 characters is recommended.
- On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Longer configuration mode prompts may be truncated.

To upgrade the Cisco IOS software on your Catalyst 4900 series switch, use this procedure:

Step 1 Download Cisco IOS Release 12.2(25)EWA from Cisco.com, and place the image on a TFTP server in a directory that is accessible from the supervisor engine that will be upgraded.

Step 2 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the **promupgrade** image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

Step 3 Download the software image into Flash memory using the **copy tftp** command.

The following example shows how to download the Cisco IOS software image **cat4500-ipbase-mz.122-25.EWA** from the remote host **172.20.58.78** to **bootflash**:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4500-ipbase-mz.122_25.EWA]?
Destination filename [cat4500-ipbase-mz.122-25.EWA]?
Accessing tftp://172.20.58.78/cat4500-ipbase-mz.122-25.EWA...
Loading cat4500-ipbase-mz.122-25.EWA from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
|!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
6923388 bytes copied in 72.200 secs (96158 bytes/sec)
Switch#
```

Step 4 Use the **no boot system flash bootflash:***file_name* command to clear the **cat4500-ipbase-mz.122-25.EWA** file and to save the BOOT variable.

The following example shows how to clear the BOOT variable:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4500-ipbase-mz.122_25.EWA
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 5 Use the **boot system flash** command to add the Cisco IOS software image to the BOOT variable.

The following example shows how to add the **cat4500-ipbase-mz.122-25.EWA** image to the BOOT variable:

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4500-ipbase-mz.122_25.EWA
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 6 Use the **config-register** command to set the configuration register to 0x2102.

The following example show how to set the second least significant bit in the configuration register:

```
Switch# configure terminal
Switch(config)# config-register 0x2102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

Step 7 Enter the **reload** command to reset the switch and load the software.

Caution No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process by performing a reset, power cycle, or OIR of the supervisor, for at least five minutes.

The following example shows the output from a successful upgrade followed by a system reset:

```
Switch# reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
Compressed configuration from 2668 bytes to 1127 bytes[OK]
Proceed with reload? [confirm]

00:02:11: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Comm
and.
```

```
 ********************************************************
 *                                                      *
 * Welcome to Rom Monitor for WS-C4948-10GE System.     *
 * Copyright (c) 1999-2005 by Cisco Systems, Inc.       *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************

 Rom Monitor Program Version 12.2(25r)EWA
 Supervisor: WS-C4948-10GE  Chassis: WS-C4948
 Hardware Revisions - Board: 8.3 CPLD Gill: 17


 MAC Address  : 00-0b-fc-ff-3b-ff
 IP Address   : 10.5.43.225
 Netmask      : 255.255.255.0
 Gateway      : 10.5.43.1
 TftpServer   : 10.5.5.5


 ***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
 . . . . .

 ******** The system will autoboot now ********


 config-register = 0x2102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4500-ipbase-mz.122-25.EWA

Rommon reg: 0x00004180
############
k2diags version 5.0.1_e

prod: WS-C4948-10GE  part: 0  serial: 0


Power-on-self-test for Module 1:  WS-C4948-10GE
 Port/Test Status: (. = Pass, F = Fail, U = Untested)

Cpu Subsystem Tests ...
seeprom: . temperature_sensor: .

Port Traffic: L2 Serdes Loopback ...
 0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
62: . 63: .


Port Traffic: L2 Asic Loopback ...
 0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
62: . 63: .


Port Traffic: L3 Asic Loopback ...
```

```
 0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: .
36: . 37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: .
62: . 63: .


Switch Subsystem Memory ...
 1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .
49: . 50: . 51: .


Front Panel Ports ...
 1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: . 12: .
13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: . 24: .
25: . 26: . 27: . 28: . 29: . 30: . 31: . 32: . 33: . 34: . 35: . 36: .
37: . 38: . 39: . 40: . 41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .


Module 1 Passed


Exiting to ios...

Rommon reg: 0x00000180
################################
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
 12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Image text-base: 0x10000000, data-base: 0x11269914
```

```
#    #    ##    #####   #    #    #    #    #   ####
#    #   #  #   #    #  ##   #    #    ##   #  #    #
#    #  #    #  #    #  # #  #    #    # #  #  #
# ## #  ######  #####   #  # #    #    #  # #  #  ###
##  ##  #    #  #   #   #   ##    #    #   ##  #    #
#    #  #    #  #    #  #    #    #    #    #   ####

The following environment variable(s) are set.  Setting these
environment variables may cause the system to behave unpredictably.
        "DontShipAllowChassisSimulation"
        "gdbEnable"
Use 'clear platform environment variable unsupported' to clear these variables.

cisco WS-C4948-10GE (MPC8540) processor (revision 3) with 262144K bytes of memor
y.
Processor board ID 0
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Uncompressed configuration from 1127 bytes to 2668 bytes

Press RETURN to get started!

00:00:06: %C4K_IOSMODPORTMAN-4-POWERSUPPLYBAD: Power supply 2 has failed or been
 turned off
00:00:06: %C4K_IOSMODPORTMAN-4-POWERSUPPLYFANBAD: Fan of power supply 2 has fail
ed
00:00:15: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:15: %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 1 (WS-C4948-10GE S/N: 0 Hw:
0.3) is online
00:00:16: %SYS-5-CONFIG_I: Configured from memory by console
00:00:16: %SYS-5-RESTART: System restarted --
Cisco IOS Software, Catalyst 4900 L3 Switch Software (cat4500-IPBASE-M), Version
 12.2(25)EWA, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 17-Aug-05 17:09 by alnguyen
Switch>
Switch#
```

Step 8 Use the **show version** command to verify that the new Cisco IOS release is operating on the switch.

Limitations and Restrictions

These sections list the limitations and restrictions for the current release of Cisco IOS software on the Catalyst 4900 series switch.

- For IP Unnumbered, the following are not supported:
  - Dynamic routing protocols
  - HSRP/VRRP
  - Static arp

  - Unnumbered interface and Numbered interface in different VRFs
- For WCCP version 2, the following are not supported:
  - GRE encapsulation forwarding method
  - Hash bucket based assignment method
  - Redirection on an egress interface (redirection out)
  - Redirect-list ACL
- For IPX software routing, the following are not supported:
  - NHRP (Next Hop Resolution Protocol)
  - NLSP
  - Jumbo Frames
- For AppleTalk software routing, the following are not supported:
  - AURP
  - AppleTalk Control Protocol for PPP
  - Jumbo Frames
  - EIGRP
- For PBR, the following are not supported:
  - Matching cannot be performed on packet lengths
  - IP precedence, TOS, and QoS group are fixed
  - ACL or route-map statistics cannot be updated
- IGRP not supported (use EIGRP, instead).
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect, as only classless routing is supported. The command **ip classless** is not supported as classless routing is enabled by default.
- Catalyst 4500 supervisor engines will not be properly initialized if the VLAN configuration in the startup file does not match the information stored in the VLAN database file. This situation might occur if a backup configuration file was used.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 128 for details on alternatives.
- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not harm your system, you might want to remove it to avoid confusion.

  Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is sample output of the **show standby GigabitEthernet1/1** command:

  ```
  switch(config)# interface g1/1
  switch(config)# no standby 0 name (0 is hsrp group number)
  ```

- For HSRP "preempt delay" to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, thereby ensuring that a hello is received before HSRP leaves the initiate state.

  Use the **standby delay reload** option if the router is rebooting after reloading the image.

- When you attempt to run OSPF between a Cisco router and a third party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

  Workaround: Since the problem is caused by mismatched MTUs, the solution is to change the MTU on either router to match the neighbor's MTU.
- The Ethernet management port on the supervisor module is active in ROMMON mode only.
- If an original packet is dropped due to transmit queue shaping and/or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- All software releases support a maximum of 16,000 IGMP snooping group entries.
- For all software releases, the CLI contains some commands that are not supported. (CSCdw44274)
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- The threshold for the Dynamic Arp Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.

  Workaround: Verify whether or not the Neighbor discovery cache has an entry, separate from regular troubleshooting areas of IPv6 address configurations and other configurations.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address will be lost.
- By default, IPv6 is not enabled. To route IPv6, you must issue the **IPv6 unicast-routing** command. If you plan to use IPv6 multicast routing, use the **IPv6 multicast-routing** command.
- By default, CEF is not enabled for IPv6 (once IPv6 unicast routing is enabled). To prevent IPv6 traffic from being process-switched, use the **IPv6 cef** command.
- Multicast sources in community VLANs are not supported.
- Two-way community VLANs are not supported.
- Voice VLANs are not supported on community VLAN host interfaces.
- Private VLAN trunks do not carry community VLANs.
- The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 1000. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.
- While configuring PVLAN promiscuous trunk ports, the maximum number of mappings is 500 primary VLANs to 500 secondary VLANs.
- 802.1X inaccessible authentication bypass feature is not supported with NAC LAN port IP feature.
- Changes to the console speed in "line console 0" configuration mode do not impact console speed in ROMMON mode. To apply the same console speed in ROMMON mode, use the "confreg" ROMMON utility and change ROMMON console speed.
- If a Catalyst 4900 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

If this message appears, check that there is network connectivity between the switch and the ACS. You should also check that the switch has been properly configured as an AAA client on the ACS.

- The **bgp shutdown** command is not supported in BGP router configuration mode. Executing this command might produce unexpected results.
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)
- Interfaces on the module WS-X4148-RJ45V may not establish a link with a Daiden DN-2800G media converter, when both the switch and the media converter interfaces are configured to operate at 100 Mbps and full duplex. This situation occurs when the interface on the module is configured to automatically detect and power up devices inline with the **power inline auto** command. This caveat is exhibited in all software releases.

  Workarounds:

  1. Disable inline power on the switch ports using the **power inline never** command.

  2. Configure the media converter to autonegotiate the speed and duplex instead of running at 100 Mbps and full duplex. (CSCee62109)
- IPSG for Static Hosts basically supports the same port mode as IPSG except that it does not support trunk port:
  - It supports Layer 2 access port and PVLAN host port (isolated or community port).
  - It does not support trunk port, Layer 3 port or EtherChannel.
- IPSG for Static Hosts should not be used on uplink ports.
- Selective DBL is only supported for non-tagged or single-tagged IP packets. To achieve Selective DBL-like functionality with a non-IP packet (like Q-in-Q and IPX), apply an input policy map that matches COS values and specifies DBL in the class map.
- For Selective DBL, if the topology involves Layer 2 Q in Q tunneling, the match cos policy map will apply to the incoming port.
- If a set of DSCP values are already configured (e.g. 0-30, 0-63), specifying a subset of these DSCP values with the **qos dbl dscp-based 0-7** command will not remove the unwanted DSCP values of 8 through 63. Rather, you must use the **no** form of the command to remove the extraneous values. In this case, the **no qos dbl dscp-based 8-63** command will leave 0-7 selected.
- If policing is performed on an input policy for a flow, the dbl used in output policies for that flow is ignored. (CSCsh60214)
- When using Port Security with Multi Domain Authentication (MDA) on an interface:
  - You must allow for at least 3 MAC addresses to access the switch: 2 for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
  - The data and voice VLAN IDs must differ.
- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may hit 100 per cent if there are a large number of hosts to learn. The CPU usage will drop once the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3,6 and 9, the violation messages are printed only for port 9.

  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts are displayed in the device tracking table as INACTIVE.
  - Autostate SVI does not work on EtherChannel.

- After the fix for CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area, but there is still a system-defined GARP class in Control Plane Policing (CPP). CPP is a macro with many CLIs and the GARP class creation CLI has been removed.
- As of Cisco IOS Release 12.2(31)SGA1, the GARP class is no longer part of the CoPP. (Due to the fix associated with CSCsg08775, even though the system-cpp-garp-range entry still appears in the CPP configuration, it is merely idling and will be removed in future releases.) Henceforward, you can manipulate GARP traffic with user ACLs and QoS. If you want to protect CPU against GARP packets, you also can "police down" GARP packets using CoPP after you define the user class for the GARP packet. (This is now possible because GARP is no longer part of the Static CAM area.)

  Due to tight integration of CPP implementation between IOS and platform code, an error message will always appear during boot-up and CPP will not be applied when downgrading IOS software from a version where this caveat is integrated to a previous release (where this fix is not present):

  ```
  %Invalid control plane policy-map; Please unconfigure policy-map attached to
  control-plane, and associated class-maps, and execute config command "macro global
  apply system-cpp" error: failed to install policy map system-cpp-policy
  ```

  As a workaround do the following:

  1. Back-up your configuration when performing software downgrading.

  2. Remove all CPP entries manually from the config and then re-appy the **macro global apply system-cpp** command.

  There should be no problem associated with this caveat while upgrading between releases (CSCsh45714).

- When ipv6 is enabled on an interface via any CLI, it is possible to see the following message:

  ```
  % Hardware MTU table exhausted
  ```

  In such a scenario, the ipv6 MTU value programmed in hardware will be different from the ipv6 interface MTU value. This will happen if there is no room in the hw MTU table to store additional values.

  You must free up some space in the table by unconfiguring some unused MTU values and subsequently disable/re-enable ipv6 on the interface or reapply the MTU configuration.

- To stop IPSG with Static Hosts on an interface, use the following commands in interface configuration submode:

  ```
  Switch(config-if)# no ip verify source
  Switch(config-if)# no ip device tracking max"
  ```

  To enable IPSG with Static Hosts on a port, issue the following commands:

  ```
  Switch(config)# ip device tracking ****enable IP device tracking globally
  Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
  Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
  ```

Caution If you only configure the **ip verify source tracking [port-security]** interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with Static Hosts will reject all the IP traffic from that interface.

Note The issue above also applies to IPSG with Static Hosts on a PVLAN Host port.

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Note All caveats in Release 12.4 also apply to the corresponding 12.4 E releases. Refer to the *Caveats for Cisco IOS Release 12.4* publication at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/124cavs/124mcavs.htm

Note For the latest information on PSIRTS, refer to the Security Advisories on CCO at the following URL: http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Open Caveats in Cisco IOS Release 12.2(40)SG

This section lists the open caveats in Cisco IOS Release 12.2(40)SG:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

This does not impact performance.

Workaround: Issue the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCse50565)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

Resolved Caveats in Cisco IOS Release 12.2(40)SG

This section lists the resolved caveats in Release 12.2(40)SG:

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

  Workaround: Issue **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362

- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

  Workaround: Issue **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362

- SNMPv3 might not work after an IOS upgrade.

  Workaround: Re-apply user credentials with the **snmp-server user** command.

Open Caveats in Cisco IOS Release 12.2(37)SG1

This section lists the open caveats in Cisco IOS Release 12.2(37)SG1:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCse50565)

- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

  Workaround: Issue **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362

- IGMP Filtering feature is not available in Cisco IOS Release 12.2(37)SG. For example, the command **igmp filter ....**, used to apply IGMP filtering on an interface, is not recognized by IOS.

  This is a temporary issue and is expected to be resolved in future IOS releases

  Workaround: None. (CSCsi40783)

Resolved Caveats in Cisco IOS Release 12.2(37)SG1

This section lists the resolved caveats in Release 12.2(37)SG1:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

  (CSCeb21064)

- Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

(CSCsd81407)

- Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:
  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

  (CSCsi60004)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

  (CSCin95836)

Open Caveats in Cisco IOS Release 12.2(37)SG

This section lists the open caveats in Cisco IOS Release 12.2(37)SG:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCse50565)

- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

  Workaround: Issue **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362

- IGMP Filtering feature is not available in Cisco IOS Release 12.2(37)SG. For example, the command **igmp filter ....**, used to apply IGMP filtering on an interface, is not recognized by IOS.

  This is a temporary issue and is expected to be resolved in future IOS releases

  Workaround: None. (CSCsi40783)

Resolved Caveats in Cisco IOS Release 12.2(37)SG

This section lists the resolved caveats in Release 12.2(37)SG:

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

  Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

  (CSCsb12598, CSCsb40304, and CSCsd92405)

- A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

(CSCsd85587)

Open Caveats in Cisco IOS Release 12.2(31)SGA5

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA5:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA5

This section lists the resolved caveats in Release 12.2(31)SGA5:

- Once auto-QoS is enabled on a switch, data traffic may be dropped when Dynamic Buffer Leaking (DBL) is enabled.

While this problem occurs, traffic drops are displayed under the Dbl-Drop-Queue counter on the output of the **show interface <mod/port> counter detail** command.

Workaround: Disable DBL globally by configuring the **no qos dbl** command. (CSCsk07525)

- When MSDP and OSPF are configured and you issue the **no ip routing** command, the switch reloads because of memory corruption in one of the pointers used by MSDP.

  To observe the problem, the MSDP timer must be set to 1.

  Workaround: Because this s problem does not occur if the MSDP timer is bigger, increase the timer to 5. (CSCsj61328)

- A Cisco network access server (NAS) may enter an infinite loop, produce CPUHOG error messages similar to the following, and then reload:

  ```
  %SYS-3-CPUHOG: Task is running for (112000)msecs, more than (2000)msecs
  (1/0),process = RADIUS
  ```

  If “radius-server retry method reorder” is not configured, the router may neglect to transmit RADIUS packets to servers after the “server-private” server if the “server-private” server does not respond. In addition, the reference count of a server, as shown by the output of the <CmdBold>debug aaa server-ref-count<noCmdBold> EXEC command, may improperly drop to zero. This results in no packets being transmitted to the server unless it is unconfigured and reconfigured.

  Workaround: None. (CSCin45879)

- Let us say that you have the following topology with private trunk links configure:

  Multicast Source---4500------Private VLAN Trunk----Switch-----STB

  When you change channels on the set top box, the IGMP leaves are not acknowledged and the traffic accumulates across the link (the link utilization increases by 4mb).

  Workaround: Remove the trunk configuration and configure the link as an access port. (CSCsl09521)

- A switch running RIP on a Cisco IOS Release after 12.3(14.8) that has **ip summary-address rip 0.0.0.0 0.0.0.0** configured on an interface, will send out the default with a metric of 16.

  Workaround: Instead of using **ip summary-address rip 0.0.0.0 0.0.0.0** to only send out the default, configure a distribute-list under the rip process. (CSCsd68016)

Open Caveats in Cisco IOS Release 12.2(31)SGA4

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA4:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  Switch# show policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)
- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

Workaround: None.

This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA4

This section lists the resolved caveats in Release 12.2(31)SGA4:

- For Cisco IOS Releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

- When trunk ports configured with VLANs associated with SVIs that are participating in a link state routing protocol come up after either a **no shutdown** or a supervisor engine switchover, log messages similar to the following may appear:

  ```
  Nov 19 05:11:02 MET: %IPC-5-WATERMARK: 1801 messages pending in rcv for
  the port CF : Standby(2020000.11) seat 2020000
  ```

  Such messages indicate that there are pending messages for active and standby supervisor engine inter-process communication. This condition does not impact switching traffic.

  Workaround: None. (CSCsg83090)

- For Cisco IOS Release 12.2(31)SG and later releases, RADIUS attribute 32 is not sent to the RADIUS server.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10. (CSCsi22041)

- An inconsistancy exists between the default signalling DSCP value used by the Catalyst 4500 series switch and CallManager 4.x, which uses DSCP 24 (by default) for the Cisco IP phone and softphone signalling. However, Auto-QoS operating on a switch requires DSCP 26. This inconsistancy causes Cisco IP phone packets to egress the switch with an incorrect DSCP. This also prevents Softphone/IP Communicator packets from obtaining the appropriate QoS.

```
Switch# show qos map cos dscp
CoS-DSCP Mapping Table
CoS: 0 1 2 3 4 5 6 7
--------------------------------
DSCP: 0 8 16 26 32 46 48 56
```

Workaround: None. (CSCsi52529)

- If multiple interfaces in the OSPF area have the same IP address (duplicate IP addresses are present in the network) and the IP address is used as a link-state ID of the network LSA, this network LSA might occur in the OSPF database with a high Age:

```
                Net Link States (Area 100)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.22.2     192.168.22.6     3391732      0x80000CCE 0x0053CD
```

  Additionally, CPU load for OSPF process might increase.

  Workaround: Avoid conflicting IP addresses. Remove duplicate IP address or shutdown the interface. (CSCsi11438)

- Lock & Key on a Catalyst 4948 switch running Cisco IOS Release 12.2(31)SGA1 does not work properly. When you open up the ACL with the **access-enable host** command, the ACL is correctly updated with an entry for the host. You can verify this with the **show access-list** command. However, the entry is not taking affect and the ACL is not permitting traffic from that IP address.

  Workaround: After entering the **access-enable host** command, remove, then reapply the ACL to the interface. (CSCsi20981)

- When a port on a Catalyst 4500 series switch is configured as a Private VLAN trunk port carrying normal and secondary VLANs, any ingress QoS policy applied to normal VLANs on that port in the ingress direction does not get programmed in the hardware. So, ingress traffic on normal VLANs cannot be policed using per-port per-VLAN input policers.

  Ingress service policies applied to secondary VLANs on that port work properly and are not affected.

  Workaround: None. (CSCsi48332)

Open Caveats in Cisco IOS Release 12.2(31)SGA3

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA3:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)
- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)
- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)
- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)
- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)
- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)
- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)
- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).
- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)
- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA3

This section lists the resolved caveats in Release 12.2(31)SGA3:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

  (CSCin95836)

Open Caveats in Cisco IOS Release 12.2(31)SGA2

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA2:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  Switch# show policy-map int
    FastEthernet3/2

     Service-policy output: p1
  ```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA2

This section lists the resolved caveats in Release 12.2(31)SGA2:

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- If two next-hop router interfaces are configured on a PBR route map, CPU utilization may be high if the first next-hop router interface is reachable via interface Null0:

  ```
  route-map PBR permit 10
    match ip address <ACL>
    set ip next-hop <NEXT-HOP 1> <NEXT-HOP 2>
  ```

  Workaround: Ensure that the next-hops *do not fall* under a route pointing to Null0. Such routes may have been entered either statically or by a routing protocol configured for summarization. (CSCsd88586)

- After a PC configured for 802.1X disconnects from an IP phone port through a Catalyst 4500 series switch, the port transitions to the guest VLAN. When a PC reconnects, the switch successfully authenticates the user but the user remains on the guest VLAN. Through the **show dot1x interface gigx/y detail** command, the state machine indicates that the port is authenticated and authorized on the guest VLAN.

  Workarounds:

  1) Disable the 802.1X guest-vlan supplicant. The port will not remain in the guest VLAN state; It will transition out of the unauthorized state.

  2) Use dynamic VLAN assignment through the ACS to assign the correct VLAN to the port.

  (CSCsh47641)

- The Catalyst 4500 switch does not set the router alert bit in multicast group-specific queries.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA2. (CSCsi74467)

- Windows XP PCs configured for machine authentication and PEAP may not receive an updated IP address from the DHCP server based on user credentials if the PC has been machine authenticated and can ping its previously assigned default gateway.

Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA10 or 12.2(31)SGA2. (CSCsi34572)

- The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

  (CSCsc19259)

Open Caveats in Cisco IOS Release 12.2(31)SGA1

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA1:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  – Use a different copy protocol.

  – Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  – A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.

  – This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  – Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.

  – Configure the correct default gateway on the host side. (CSCse75660)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCse50565)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA1

This section lists the resolved caveats in Release 12.2(31)SGA1:

- The Catalyst 4900 switch running 12.2(31)SG and configured for 802.1X may reset after displaying the following console messages while switching EAP packets:

```
Jul 27 08:14:36: %SYS-2-FREEFREE: Attempted to free unassigned memory at 1A35ACA8,
alloc 10355D60, dealloc 103594B4
-Traceback= 10FAC5A8 1035A150 1035A30C 105A7A7C 1059F3A8
Jul 27 08:14:36: %SYS-6-MTRACE: mallocfree: addr, pc
 1A35ACA8,1035A14C 195FECAC,103592E8 1A1A97D4,60000010 1A1A9780,10359134
 1A084698,10249D60 1A16F008,10355724 1A0FBE24,10359098 127B42B8,600000F8
Jul 27 08:14:36: %SYS-6-MTRACE: mallocfree: addr, pc
 127B3E80,103594C4 1A35AF4C,600000F2 1A35ACA8,103594B4 1A1F9F6C,1083D310
 127B16CC,6000005E 127B11A8,50000208 127B15E0,1083D300 1A17258C,1083D2E4
Jul 27 08:14:36: %SYS-6-BLKINFO: Attempt to free a block that is in use blk 1A35AC80,
 words 580, alloc 10355D60, Free, dealloc 103594B4, rfcnt 0
-Traceback= 10F96808 10FAC5B8 1035A150 1035A30C 105A7A7C 1059F3A8
Jul 27 08:14:36: %SYS-6-MEMDUMP: 0x1A35AC80: 0xAB1234CD 0x390000 0x1983C854 0x11F30330
Jul 27 08:14:36: %SYS-6-MEMDUMP: 0x1A35AC90: 0x10355D60 0x1A35B130 0x1A35AC38 0x244
```

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA1 or later. (CSCsf09339)

- If you configure ISIS/IPv6 with the **passive-interface default** and **no passive-interface <interface>** commands, ISIS IIH advertisements will be sent from such interfaces without the local IPv6 address, preventing the formation of adjacencies.

  Workaround: Remove **passive-interface** commands from the **router isis** configuration. (CSCei21664)

- GARP-based protocol packets leak through an STP block, potentially leading to a GARP storm in a redundant topology.

  Workaround: Use Hardware Control Plane Policing (CoPP) to police GARP packets. (CSCsg08775)

- Configuring an ACL on a port configured with the **switchport access vlan dynamic** command will restart the Catalyst 4900 series switch.

  This issue impacts Catalyst 4900 series switches running IOS releases including and earlier than 12.2(31)SGA and 12.2(25)EWA6.

  Workaround: None. (CSCsg03745)

- The HSRP Active-Router does not respond to ARP requests for the virtual IP (VIP) address. Issuing **clear arp** on the HSRP standby router does not resolve the problem. This problem may occur when the same HSRP VIP address exists on different HSRP groups on different routers.

  Workaround: Issue the **no standby redirects** command. (CSCsd80754)

- When you remove the **radius-server source-ports 1645-1646** default command, the switch sends the RADIUS requests with the wrong source port, causing failed authentication attempts.

  Reloading the switch will solve the problem. Upon boot-up, **radius-server source-ports 1645-1646** will be in the running-config and communication with the RADIUS server will resume

  Workaround: Ensure the **radius-server source-ports 1645-1646** command is configured. (CSCsh22161)

- Spurious memory accesses may occur when OSPF routing is configured and UDP traffic is flooded.

  Workaround: None. (CSCsd11631)

- When a switch port is disabled and enabled, the adjacent switch port may drop up to 20 packets.

  Workaround: None. (CSCsg02099)

- QoS markings are not retained when using per-port per-VLAN QoS and IP Source Guard.

  Workaround: Disable and enable QoS. (CSCsg75348)

- The switch may reset after a PVLAN trunk port receives a high number of IGMP report messages.

  Workaround: Disable the PVLAN trunk port. (CSCsg46891)

- A switch configured in Rapid PVST spanning tree mode will not automatically recover an interface that was placed into ROOT_Inc state by ROOT guard.

  Workaround: Bounce any interface on the 4900 switch causing a spanning tree topology change. (CSCsc95631)

- A tftp client that attempts to transfer a file from an IOS device configured as a tftp server, and which is denied by an ACL, receives a result that depends on whether the file is being offered for download. This may allow a third party to enumerate which files are available for download.

  Workaround: Apply one of the following:

1. Interface ACL - Configure and attach an access list to every active router interface configured for IP packet processing. Once enabled, the tftp server in IOS listens by default on all interfaces enabled for IP processing. So, the access list needs to deny traffic to every IP address assigned to an active router interface.

2. Control Plane Policing - Configure and apply a CoPP policy.

Note CoPP is only available on certain platforms and IOS release trains. Additional information on the configuration and use of the CoPP feature can be found at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a00802 11f39.shtml

3. Infrastructure ACLs (iACL) - Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and to block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for iACLs (:http://www.cisco.com/warp/public/707/iacl.html).

4. Receive Access Lists (rACLs) - The rACLs protect a device from harmful traffic before the traffic can impact the route processor. rACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets (:http://www.cisco.com/warp/public/707/racl.html). (CSCse04560)

Note The suggested workarounds are an "all or nothing" solution. While the tftp-server feature in IOS allows per-file ACLs to be attached to every file being offered for download, the suggested workarounds are global. They will either prevent or allow access to all files that are being shared. You should apply a workaround in addition to the existing per-file ACLs, instead of replacing them.

- Test and debug commands are not available in cryptographic images.

  Workaround: None. (CSCse61081)

- If port security is enabled on a PVLAN isolated trunk port, Layer 3 connectivity to hosts connected via that port may be unreachable.

  Workaround: None. (CSCsg11229)

- A Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA6 might drop an ARP request. The switch cannot resolve the MAC address of connected devices.

  This problem is not seen with Cisco IOS Releases 12.2(25)EWA4 and 12.2(25)EWA5.

  Workaround: None. (CSCsf16422)

- When your DHCP address lease time is not updated on a switch configured with IP Source Guard, you cannot renew your DHCP IP addresses. Your non-DHCP traffic is dropped and the following error message is logged:

  ```
  %IP_SOURCE_GUARD-4-IP_SOURCE_GUARD_DENY_PACKET: IP Source Guard detects and drops
  illegal traffic
  ```

  Workaround: Disable and enable the affected switch ports. (CSCsd65833)

- When you configure a switch with an IEEE 802.1X Failed Authentication VLAN and IEEE 802.1X supplicants use tunneled EAP methods such as PEAP and EAP-TLS for authentication, the switch attempts to send an EAP Success message on the third consecutive failed authentication attempt rather than an EAP Failure message. This results in erratic supplicant and network behavior.

  Workaround: Either do not use tunneled EAP methods or disable the authentication failed VLAN. (CSCse71105)

- When the VTP configuration revision is higher than 0x7FFFFFFF (2147483647), the configuration revision displays in the output of the **show vtp status** command as a negative number.

  Workaround: Reset the VTP domain name for all switches in the domain. (CSCse40078)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

  (CSCsd75273)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

  (CSCse52951)

- A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

(CSCsd85587)

Open Caveats in Cisco IOS Release 12.2(31)SGA

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
```

```
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA

This section lists the resolved caveats in Release 12.2(31)SGA:

- A Catalyst 4900 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- When running Cisco IOS Release 12.2(25)EWA6 on a Catalyst 4948 series switch, or the Catalyst 4013+TS supervisor engine and the 4306-GB-T linecard, the following problems may be seen on RJ45 ports only:

  - When sending packets of size greater than 6656 bytes, the ports cannot sustain the linerate when operating at 1Gbps. However, they can sustain the linerate for packet sizes less than or equal to 6656 bytes when operating at 1Gbps.
  - Occasionally, the TxQueue's associated with the RJ45 ports may get stuck when packets greater than 6656 bytes and the port is operating in either 10Mbps or 100Mbps or 1Gbps. You would see messages like the following:

    ```
    Aug  1 04:46:01 CDT: %C4K_HWPORTMAN-4-BLOCKEDTXQUEUE: Blocked transmit queue
    HwTxQId1 on Switch Phyport Gi1/35, count=1784
    Aug  1 04:46:12 CDT: Current Freelist count 5629. Fell below threshold 601 times
    consecutively
    Aug  1 04:46:42 CDT: Current Freelist count 5629. Fell below threshold 1202 times
    consecutively
    ```

  Workaround: Use packets sizes less than or equal to 6656 bytes or use Cisco IOS Release 12.2(25)EWA5 until the fix is available in Cisco IOS Release 12.2(25)EWA8. (CSCse29295)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

(CSCek26492)

- The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

  (CSCek37177)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

  (CSCsd58381)

- A Cisco router may drop a TCP connection to a remote router.

  When an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than the remote router can handle, the router might advertise a zero window. So, when the router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends. On the Cisco router, enter the **ip tcp window-size** command. When you use a Telnet connection, reduce the **screen-length** argument in the **terminal length** command to 20 or 30 lines. (CSCsc39357)

Open Caveats in Cisco IOS Release 12.2(31)SG2

This section lists the open caveats in Cisco IOS Release 12.2(31)SG2:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)
- A Catalyst 4900 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)
- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

  (CCSCsd34759)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG3

This section lists the resolved caveats in Release 12.2(31)SG3:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

Open Caveats in Cisco IOS Release 12.2(31)SG2

This section lists the open caveats in Cisco IOS Release 12.2(31)SG2:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- A Catalyst 4900 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if

QueueID	Old QueueName	New QueueName
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

  (CCSCsd34759)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG2

This section lists the resolved caveats in Release 12.2(31)SG2:

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

  (CSCin95836)

Open Caveats in Cisco IOS Release 12.2(31)SG1

This section lists the open caveats in Cisco IOS Release 12.2(31)SG1:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- A Catalyst 4900 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

  (CCSCsd34759)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG1

This section lists the resolved caveats in Release 12.2(31)SG1:

- Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Because CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

  Workaround: Disable on interfaces where CDP is not necessary. (CSCse85200)

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

Open Caveats in Cisco IOS Release 12.2(31)SG

This section lists the open caveats in Cisco IOS Release 12.2(31)SG:

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  Switch# show policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)
- A Catalyst 4900 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)
- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG and later releases.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)
- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

  (CCSCsd34759)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG

This section lists the resolved caveats in Release 12.2(31)SG:

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

Open Caveats in Cisco IOS Release 12.2(25)SG4

This section lists the open caveats in Cisco IOS Release 12.2(25)SG4:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)
- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(25)SG4

This section lists the resolved caveats in Release 12.2(25)SG4:

- In Cisco IOS Release 12.2(33)SXH or 12.2(18)SXF10, the output of the **show pagp neighbor** command may truncate the neighbor device name and port name fields by 1 character. This is a display issue and has no functional impact on the PAGP protocol.

  Workaround: None. If you want to determine a partner's correct information, use the **show cdp neighbor** command.

  (CSCsj81502)

Open Caveats in Cisco IOS Release 12.2(25)SG3

This section lists the open caveats in Cisco IOS Release 12.2(25)SG3:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)
- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)
- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)
- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(25)SG3

This section lists the resolved caveats in Release 12.2(25)SG3:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

Open Caveats in Cisco IOS Release 12.2(25)SG2

This section lists the open caveats in Cisco IOS Release 12.2(25)SG2:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  Switch# show policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(25)SG2

This section lists the resolved caveats in Release 12.2(25)SG2:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml.

(CSCef77013)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

  (CSCin95836)

Open Caveats in Cisco IOS Release 12.2(25)SG1

This section lists the open caveats in Cisco IOS Release 12.2(25)SG1:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

    Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(25)SG1

This section lists the resolved caveats in Release 12.2(25)SG1:

- Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Because CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

Workaround: Disable on interfaces where CDP is not necessary. (CSCse85200)

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

  (CSCsd75273)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

  (CSCse52951)

Open Caveats in Cisco IOS Release 12.2(25)SG

This section lists the open caveats in Cisco IOS Release 12.2(25)SG:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  Switch# show policy-map int
    FastEthernet3/2
  ```

```
Service-policy output: p1

  Class-map: c1 (match-all)
    0 packets<--------It stays at '0' despite of traffic being received
    Match: access-group name fnacl21
    police: Per-interface
      Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(25)SG

This section lists the resolved caveats in Release 12.2(25)SG:

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command. (CSCsa67042)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

Open Caveats in Cisco IOS Release 12.2(25)EWA13

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA13:

- While configuring Smartport macros via HTTP interactively, a switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser *command* area as if you were entering the commands through the CLI. (CSCei76082)

- A switch upgrading to Cisco IOS Releases 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This caveat is cosmetic only; it does not impact the operation of the switch.

  Workaround: Power-cycle the switch. (CSCsg00796)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA13

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA13:

- Once auto-QoS is enabled on a switch, data traffic may be dropped when Dynamic Buffer Leaking (DBL) is enabled.

  While this problem occurs, traffic drops are displayed under the Dbl-Drop-Queue counter on the output of the **show interface <mod/port> counter detail** command.

  Workaround: Disable DBL globally by configuring the **no qos dbl** command. (CSCsk07525)

- When MSDP and OSPF are configured, the MSDP timer is set to 1, and you issue the **no ip routing** command, the switch reloads because of memory corruption in one of the pointerrs used by MSDP.

  The caveat does not occur if the MSDP timer is greater than 1.

  Workaround: Increase the MSDP timer to 5. (CSCsj61328)

Open Caveats in Cisco IOS Release 12.2(25)EWA12

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA12:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4500 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4500 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4500 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA12

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA12:

- If a switch has a redundant supervisor, under rare conditions you will observe the following situation: You first observe the *keepalive missing* warning messages. Then, after the keepalive protocol times out, a switchover to the standby supervisor engine occurs. **4500 only**

  This happens because the active and standby supervisor engines refer to the same seed metric for calculating the EOBC collision back off timer. Consequently, the EOBC channel might get locked in infinite collisions.

  Workaround: Upgrade the software to either:

  - Cisco IOS Release 12.2(31)SGA2 and higher, or
  - Cisco IOS Release 12.2(37)SG and higher

  (CSCsh44170)

- When connecting an end device installed with Intel 82471 to a 10/100/1000BaseTX port on a Catalyst 4948 switch with both sides (the switch port and the end device) set to auto, the speed downshifts from 1000 to 100 in autonegotiate mode when the switch side reloads and the end device is *still alive* (powered on and functional).

  The problem is not observed if the third party device reloads while the switch is *still alive*.

  Workaround: Enter the **shutdown** command followed by a **no shutdow**n command on the switch port. (CSCsk54053)

- On a Cisco router that functions as an ISR configured for OSPF, shortly after OSPF adjacencies come up, the router crashes because of a bus error.

  Workaround: Either enter the **area 0** command in the OSPF VRF process or enter the **no capability transit** command in the OSPF VRF process. (CSCsi84089).

- On a Catalyst 4948 switch running Cisco IOS Release 12.2(31)SGA, after removing and reinserting the fiber cable into the SFP, the link may not come up immediately.

  Workaround: Either remove and reinsert the SFP or issue a **shutdown** command followed by the **no shutdown** command on the affected Catalyst 4948 interface. CSCsj67573

- When you add the **ip ssh ver 2** command to the configuration of the primary supervisor engine and you *fail over* to the secondary supervisor engine, the command is present in the configuration of the secondary supervisor engine. However, when you *fail back* to the primary supervisor engine, the command disappears from the configuration of the primary supervisor engine, affecting your SSH sessions.

  Workaround: None. (CSCsj51666)

Open Caveats in Cisco IOS Release 12.2(25)EWA11

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA11:

- While configuring Smartport macros via HTTP interactively, a switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- If you upgrade a switch to Cisco IOS Releases 12.2(25)EWA or 12.2(31)SG, it might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A switch running Cisco IOS Release 12.(25)EWA8 and beyond will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- A switch might experience high CPU utilization due to the Cat4k Mgmt LoPri process and the K2CpuMan and K2L2 Address Table reviews (using the **show platform health** command.

  High CPU utilization does not impact the traffic switched in hardware.

  The problem is seen when a large MAC address table exists and when the switch is frequently relearning MAC addresses on multiple VLANs. Enabling the **service internal** command followed by the **debug platform log feature k2l2addresstable** command will display output similar to the following:

Note Do not enable these commands on a production switch unless instructed by Cisco TAC.

```
*Nov 13 12:56:32.066 CLT-1: K2L2AddressTableMan::newEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.030 CLT-1: K2L2AddressTableMan::deleteEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.046 CLT-1: K2L2AddressTableMan::newEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.062 CLT-1: K2L2AddressTableMan::deleteEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
```

Workaround: None. (CSCsg76868)

- When the console port of a Catalyst 4948 is connected to a serial port on a Cisco 3845 router NM-32A or NM-16A module, the ASYNC LED of a NM module is off. The Catalyst 4948-10GE chassis is not affected.

  Workaround: None. (CSCsj43019)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA11

This section lists the resolved caveat in Cisco IOS Release 12.2(25)EWA11:

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Open Caveats in Cisco IOS Release 12.2(25)EWA10

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA10:

- While configuring Smartport macros via HTTP interactively, a switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- If you upgrade a switch to Cisco IOS Releases 12.2(25)EWA or 12.2(31)SG, it might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A switch running Cisco IOS Release 12.(25)EWA8 and beyond will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  – Remove dot1x from the port.

  – Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- A switch might experience high CPU utilization due to the Cat4k Mgmt LoPri process and the K2CpuMan and K2L2 Address Table reviews (using the **show platform health** command.

  High CPU utilization does not impact the traffic switched in hardware.

  The problem is seen when a large MAC address table exists and when the switch is frequently relearning MAC addresses on multiple VLANs. Enabling the **service internal** command followed by the **debug platform log feature k2l2addresstable** command will display output similar to the following:

Note Do not enable these commands on a production switch unless instructed by Cisco TAC.

```
*Nov 13 12:56:32.066 CLT-1: K2L2AddressTableMan::newEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.030 CLT-1: K2L2AddressTableMan::deleteEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.046 CLT-1: K2L2AddressTableMan::newEntry index 55620 vlan 1010
address 00:D0:02:2D:38:1A
*Nov 13 12:56:34.062 CLT-1: K2L2AddressTableMan::deleteEntry index 61956 vlan 1020
address 00:D0:02:2D:38:1A
```

  Workaround: None. (CSCsg76868)

- When the console port of a Catalyst 4948 is connected to a serial port on a Cisco 3845 router NM-32A or NM-16A module, the ASYNC LED of a NM module is off. The Catalyst 4948-10GE chassis is not affected.

  Workaround: None. (CSCsj43019)

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA10

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA10:

- If IGMP snooping and multicast routing are configured on a switch, and the switch is acting as a group querier and receives an IGMP group-specific query, the switch clears the entry from its IGMP group membership table after two seconds.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA2 or 12.2(25)EWA10. (CSCsh65870)

- Windows XP PCs configured for machine authentication and PEAP may not receive an updated IP address from the DHCP server based on user credentials if the PC has been machine authenticated and can ping its previously assigned default gateway.

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA10 or 12.2(31)SGA2. (CSCsi34572)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

- For switches running IOS software prior to Release 12.2(25)EWA10, DHCP snooping syslog statistics may not be sufficient for some debugging scenarios.

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA10. (CSCsg91116)

- On PoE line cards connected to IP phones or other PoE networking devices, you might see a S2W console warning message indicating that the POE devices are either not responding to polling from the supervisor or the devices are in an error state. When this situation exists, PoE service may not work correctly. For instance, phones will not have power or power will be removed intermittently from some ports.

  This might happen for the following reasons:

  – There is a marginal and/or failing component(s) on the line card (requires RMA and EFA).

  – The hardware and software states are not synchronized due to a power *glitch* or to a reset of the -48V PoE.

  This situation occurs on Cisco IOS Release 12.2(31)SGA1 or lower (except for Cisco IOS Release 12.2(25)EWA10).

Note This situation does not exist on the WS-X4148-RJ45V.

  Workaround: Download an image that supports PoE Health Monitoring such as Cisco IOS Release 12.2(37)SG, 12.2(31)SGA2, or 12.2(25)EWA10. These software images have code that will monitor, detect, and attempt to correct random S2W errors. Although this code does not prevent the problem, it will positively identify the issue and reduce recovery time.

  If you experience three HealthCheck warning messages within a week, RMA the line card immediately, and request an Engineer Failure Analysis (EFA) report. Perform the following debugging steps if your IP phone or PoE device fails:

Step 1 Determine if the IP phone works using other ports on the same line card.

Step 2 Determine if the same IP phone works using another line card(s) within the switch.

Step 3 Capture **show tech-support** and **show platform chassis module** *module*.

Step 4 Reset the linecard by issuing **hw-module module** *module* **reset** or by removing and reinserting the line card. Determine if the IP phone receives power from the switch.

Step 5 Capture **show tech-support** and **show platform chassis module** *module*.

Step 6 RMA the line card if the problem persists with RMA. Ask the TAC engineer to create an EFA.

(CSCsf26804)

- Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml.

  (CSCef77013)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

  (CSCin95836)

- The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

(CSCsc19259)

Open Caveats in Cisco IOS Release 12.2(25)EWA9

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA9:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4900 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4900 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4900 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4900 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA9

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA9:

- When you telnet to a switch and configure the **autocommand-options nohangup** command on line vty 0 4, it will disappear once you exit. (If you look at the running configuration from the console connection, the command is not present.) This does not impact vty 5 15.

  Workaround: Open 6 telnet sessions. (CSCsg41842)

- When UDP Small Servers is enabled on an HSRP active router and it receives a UDP ECHO to the virtual ip address, the router fails to echo back by LOOPPAK.

  Workaround: None. (CSCsh13542)

- If you resume another Secure Shell (SSH) session after disconnecting an SSH session, the client console or vty will not respond until the server disconnects the session.

  Workaround: None. (CSCsd76601)

- While either initiating a Secure Shell (SSH) session from a router or copying a file to/from the router via SCP, a router may reload due to software forced crash.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash displaying the %SYS-2-WATCHDOG message:

  ```
  *Mar 29 11:29:35.938: %SYS-3-CPUHOG: Task is running for (128004)msecs, more
  than (2000)msecs
  (1426/5),process = Virtual Exec.
  -Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768
  0x41BA7490 0x41BA7750
  0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8
  0x41834200

  *Mar 29 11:29:35.942: %SYS-2-WATCHDOG: Process aborted on watchdog timeout,
  process = Virtual Exec.
  -Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490
  0x41BA7750 0x41BAC854
  0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200
  0x418341E4

  %Software-forced reload
  ```

  Workaround: Do not initiate SSH or SCP sessions from the router. (CSCsb54378)

- When you remove the **radius-server source-ports 1645-1646** default command, the switch sends the RADIUS requests with the wrong source port, causing the authentication attempts to fail.

  Workaround: Ensure that the **radius-server source-ports 1645-1646** command is configured and reload the switch. Upon boot-up, the command will be in the running-config and communication with the RADIUS server will resume. (CSCsh22161)

- Memory corruption may occur if a EIGRP stub with static routes is configured on the switch, causing the switch to crash. Symptoms include console messages similar to the following:

  ```
  Aug 23 15:43:45: %SYS-2-BADSHARE: Bad refcount in mem_lock, ptr=43258E68,
  count=FFFF8000

  Traceback= 409201A8 4007AE28 40A1D418 40A2263C 40A24610 40A25600 40C309D4 40C30D74
  40C3CBB0CMD:
  ```

  Workaround: Unconfigure the EIGRP stub with static routes. (CSCef26340)

- A memory leak may occur if a switch is configured as a RADIUS client and receives invalid RADIUS packets. The switch will not have enough packet memory to receive incoming ARP packets destined for the CPU, and ARP entries will be incomplete.

  Workaround: Disable the port that is receiving invalid RADIUS packets. (CSCeh84727)

- If the ACL configured on an SVI is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA and resize the TCAM with the **access-list hardware region balance** command to support the ACL. Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

(CSCsb12598)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

  Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

  (CSCsb40304)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

(CSCsd92405)

Open Caveats in Cisco IOS Release 12.2(25)EWA8

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA8:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4900 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4900 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4900 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4900 series switch running Cisco IOS Release 12.(25)EWA8 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- Reconfiguring a heavily-used policy map on a Catalyst 4900 series switch may cause the switch to crash. This issue affects Cisco IOS Releases 12.2(25)EWA3, 12.2(25)EWA4, 12.2(25)EWA5, 12.2(25)EWA6, 12.2(25)SG and 12.2(31)SG.

  Workaround: Remove the policy-map from all interfaces before reconfiguring its contents. (CSCse80948)

- Configuring an ACL and issuing the switchport access vlan dynamic command on a port at the same time will crash Catalyst 4900 series switches.

  This issue impacts Catalyst 4900 series switches running Cisco IOS Release 12.2(31)SGA back to at least Cisco IOS Release 12.2(25)EWA.

  Workaround: None. (CSCsg03745)

- If the ACL configured on an SVI is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA and resize the TCAM with the **access-list hardware region balance** command to support the ACL. Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA8

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA8:

In a switch running Cisco IOS Release 12.2(25)EWA8, the following symptoms might be observed.

- ARP does not resolve for directly- connected devices, impacting connectivity and preventing routing protocols from forming an adjacency.
- If UDLD “aggressive” is enabled, ports will err-disable due to UDLD, causing messages like the following to display:

```
%UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface Gi3/1, unidirectional link
detected
%PM-4-ERR_DISABLE: udld error detected on Gi3/1, putting Gi3/1 in err-disable
state
```

Note Because UDLD is merely a symptom of the problem rather than the cause, disabling UDLD will not solve the problem.

- Slow memory leak, causing messages (with tracebacks) like the following to display:

```
%SYS-2-MALLOCFAIL: Memory allocation of 784 bytes failed from 0xXXXXXX, alignment
8
Pool: Processor  Free: 36  Cause: Not enough free memory Alternate Pool: None
Free: 0  Cause: No
Alternate pool -Process= "<Process_name>", ipl= 0, pid= 49 -Traceback=
0xXXXXXX
```

Messages such as the following would be seen on the console

```
%% Low on memory; try again later
```

If one of the symptoms is observed, capture an output of the **show tech** command along with 4-5 snapshots of the following commands (over a 10 minute interval) and open a TAC Service request:

- **show plat cpu packet driver**
- **show plat cpu pack stat**
- **show platform health**
- **show mem summary**
- **show process memory**

Workaround: "Move" to Cisco IOS Release 12.2(25)EWA6. (CSCsh25687)

- Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

  By default, the Cisco IOS configuration command uses United States standards for daylight savings time rules:

  clock summer-time *zone* **recurring**

  The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March, and it changes the end date from the last Sunday of October to the first Sunday of November.

  Workaround: Use the **clock summer-time** command to manually configure the proper start and end date for daylight savings time. After the summer-time period for calendar year 2006 ends, you can configure the following for the US/Pacific time zone:

  clock summer-time *PDT* **recurring** *2 Sun Mar 2:00 1 Sun Nov 2:00*

  (CSCsg70355)

Note Using NTP is not a workaround to this problem, because it does not carry any information about timezones or summertime.

Open Caveats in Cisco IOS Release 12.2(25)EWA7

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA7:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4900 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- A Catalyst 4900 series switch upgrading to IOS versions 12.2(25)EWA or 12.2(31)SG might show unusual uptime in the output of the **show version** command:

  ```
  Switch uptime is 113 years, 43 weeks, 4 days, 7 hours, 53 minutes
  ```

  This does not impact the operation of the Catalyst 4900 series switch, appearing to be strictly cosmetic.

  Workaround: Power-cycle the switch. (CSCsg00796)

- A Catalyst 4900 series switch running Cisco IOS Release 12.(25)EWA7 will send in dot1q tagged cdp packets when dot1x is enabled on a voice VLAN port. This might cause gigabit IP phones to send in packets that are untagged, moving the phone into the data VLAN.

  Workaround: Do either of the following:

  - Remove dot1x from the port.
  - Upgrade the IOS image to Cisco IOS 12.2(31)SGA or later.

  (CSCsg10135)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- Reconfiguring a heavily-used policy map on a Catalyst 4900 series switch may cause the switch to crash. This issue affects Cisco IOS Releases 12.2(25)EWA3, 12.2(25)EWA4, 12.2(25)EWA5, 12.2(25)EWA6, 12.2(25)SG and 12.2(31)SG.

  Workaround: Remove the policy-map from all interfaces before reconfiguring its contents. (CSCse80948)

- Configuring an ACL and issuing the switchport access vlan dynamic command on a port at the same time will crash Catalyst 4900 series switches.

  This issue impacts Catalyst 4900 series switches running Cisco IOS Release 12.2(31)SGA back to at least Cisco IOS Release 12.2(25)EWA.

  Workaround: None. (CSCsg03745)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA7

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA7:

- When VRF Packet Leaking is configured on a Catalyst 4900 series switch with a Supervisor Engine IV, a packet loss of 50 per cent occurs when you ping a Catalyst 4900 series switch VRF interface IP address from a device in the global table.

  Packets forwarded by Catalyst 4900 series switch are not impacted.

  Workaround: None. (CSCej36831)

- On a Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA5, after reloading an "ip ftp source-interface <physical port>" configuration, it is impossible to upload the configuration to the FTP Server with the **copy running-config ftp** command.

  Workaround: Issue the **ip ftp source-interface <loopback port>** command rather than the **ip ftp source-interface <physical port>** command. (CSCsd22662)

- Reconfiguring a heavily-used policy map on a Catalyst 4900 series switch may cause the switch to crash. This issue affects Cisco IOS Releases 12.2(25)EWA3, 12.2(25)EWA4, 12.2(25)EWA5, 12.2(25)EWA6, 12.2(25)SG and 12.2(31)SG.

  Workaround: Remove the policy-map from all interfaces before reconfiguring its contents. Also ensure that no configuration is made in parallel that might result in concurrent modification of configured interface's state. (CSCse80948)

- Configuring an ACL on a port of a Catalyst 4900 series switch configured with the **switchport access vlan dynamic** command will cause the switch to crash.

This issue impacts switches running IOS releasse including and prior to 12.2(31)SGA and 12.2(25)EWA6.

Workaround: None. (CSCsg03745)

- GARP-based protocol packets leak through the STP block. In a redundant topology, this might lead to a GARP storm.

  Workaround: Use Hardware Control Plane Policing (CoPP) to police GARP packets. (CSCsg08775)

- When the **clear arp snmp** command is sent to a Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA4, the switch may reset.

  This issue impacts running IOS releases including and prior to 12.2(31)SG and 12.2(25)EWA6.

  Workaround: None. (CSCse49277)

- When there are a number of non-RPF multicast groups and the incoming rate of multicast traffic is high, the Catalyst 4900 series switch does not trigger a PIM Assert for some multicast groups immediately after receiving multicast packets on non-RPF interface.

  Workaround: None. (CSCse56839)

- While running Cisco IOS Release 12.2(25)EWA6 on the Catalyst 4900 series switch, the 4013+TS supervisor engine, or the 4306-GB-T linecard, you might experience the following problem on RJ45 ports:

  – When sending packets of size greater than 6656, the ports cannot sustain the linerate when operating at 1Gbps. However, they can sustain the linerate when packet sizes are less than 6656 bytes when operating at 1Gbps.

  – In rare situations, the TxQueue's associated with the RJ45 ports may get stuck when the packets of size greater than 6656 bytes are involved and the port is operating in 10Mbps, 100Mbps, or 1Gbps. Messages such as following would be seen:

  ```
  Aug  1 04:46:01 CDT: %C4K_HWPORTMAN-4-BLOCKEDTXQUEUE: Blocked transmit queue
  HwTxQId1
  on Switch Phyport Gi1/35, count=1784
  Aug  1 04:46:12 CDT: Current Freelist count 5629. Fell below threshold 601 times
  consecutively
  Aug  1 04:46:42 CDT: Current Freelist count 5629. Fell below threshold 1202 times
  consecutively
  ```

  Workaround: Use packets sizes less than or equal to 6656 bytes or use Cisco IOS Release 12.2(25)EWA5 until the fix is available in subsequent releases. The fix will be available in 12.2(25)EWA7 release onwards. (CSCse29295)

- If a Catalyst 4900 series switch running Cisco IOS Release 12.2(31)SG is configured with Port Security and Cisco IP Phones are connected to the switchports, the CPU might be higher than expected. In the output of the **show platform health** command, the process hogging the CPU would be the following:

  ```
  CAT4506#sh platform health | inc K2L2 Address
  K2L2 Address Table R   2.00  27.08     12      5  100  500   15  23   19  4871:26
  CAT4506##sh platform health | inc K2L2 Address
  K2L2 Address Table R   2.00  34.92     12      5  100  500   38  25   19  4871:32
  ```

  This process should not cause any forwarding issues.

  Workaround: None. (CSCse72353)

- Reading the object dot1dTpLearnedEntryDiscards always returns zero.

  Workaround: None. (CSCse66318)

- Applying an ACL to a Layer 3 interface on a Catalyst 4900 series switch that is too large to fit entirely in the TCAM, might cause valid arp replies to be installed incorrectly.

  Workaround: Determine which portion of the TCAM is becoming saturated and resize it accordingly. This can be done by looking at the output of the **show plat hard acl statistics u brief** command:

```
                          Entries/Total(%)  Masks/Total(%)
                            ----------------  --------------
Input  Acl(PortAndVlan)      5 / 8112 (  0)     3 / 1014 (  0)
Input  Acl(PortOrVlan)    8105 / 8112 ( 99)  1014 / 1014 (100)
Input  Qos(PortAndVlan)      0 / 8128 (  0)     0 / 1016 (  0)
Input  Qos(PortOrVlan)       0 / 8128 (  0)     0 / 1016 (  0)
Output Acl(PortAndVlan)      0 / 8112 (  0)     0 / 1014 (  0)
Output Acl(PortOrVlan)       5 / 8112 (  0)     3 / 1014 (  0)
Output Qos(PortAndVlan)      0 / 8128 (  0)     0 / 1016 (  0)
Output Qos(PortOrVlan)       0 / 8128 (  0)     0 / 1016 (  0)
```

  With Cisco IOS Release 12.2(31)SG or later you can reize the tcam allocation using the **access-list hardware region** [**feature/qos**] **in balance** [*percentage*] command. (CSCse53198)

- Upon reloading a Catalyst 4900 series switch configured with the **ip ftp source-interface** command and running Cisco IOS Release 12.2(25)EWA5, it is impossible to upload a configuraton to the FTP Server by issuing the **copy running-config ftp** command.

  Workaround: Issue the **ip ftp source-interface** <*loopback port*>, instead of the **ip ftp source-interface** <*physical port*> command. (CSCsd22662)

- A Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA6, drops some ARP request packets in some VLANs.

  Workaround: None. (CSCsf16422)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

  (CSCsd75273)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

  (CSCse52951)

Open Caveats in Cisco IOS Release 12.2(25)EWA6

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA6:

- While configuring Smartport macros via HTTP interactively, a Catalyst 4900 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- When VRF Packet Leaking is configured on a Catalyst 4900 series switch with a Supervisor Engine IV, a packet loss of 50 per cent occurs when you ping a Catalyst 4900 series switch VRF interface IP address from a device in the global table.

  Packets forwarded by Catalyst 4900 series switch are not impacted.

  Workaround: None. (CSCej36831)

- While running Cisco IOS Release 12.2(25)EWA5, after reloading an "ip ftp source-interface <physical port>" configuration, it is impossible to upload the configuration to the FTP Server with the **copy running-config ftp** command.

  Workaround: Issue the **ip ftp source-interface <loopback port>** command rather than the **ip ftp source-interface <physical port>** command. (CSCsd22662)

- When a third-party device is connected to a 1000BaseX interface and the link is shutdown/unshutdown, the autonegotiation process takes considerable time to complete and the link needs several minutes to come up again.

  Workaround: Disable autonegotiation or flow-control. (CSCse33607)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA6

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA6:

- Occasionally, when a Catalyst 4900 series switch is in VTP client mode and “switchport trunk prunning vlan none” is configured on the trunk port, the trunk interface fails to send VLAN joins to the VTP server. Some of the VLAN is pruned on the link to the VTP server even when those VLANs are used.

  Workaround: Instead of using the "none" option, provide a specific VLAN when enabling VTP pruning on the trunk interface. (CSCei42957)

- After you initially boot a Catalyst 4900 series switch, if the input interface is in PIM dense mode, “s,g” multicast cast traffic is not forwarded to the intended destination even if that group is represented by a “*,g” on the system.

  Workaround: Issue the **clear ip mroute *** command multiple times. (CSCsb50317)

- When PVLAN features (for example, PVLAN QoS) are applied on a trunk port for a number of VLANs and later removed from some VLANs, the features may be reprogrammed for all other VLANs. While the reprogramming is in progress, you might see some log message indicating that the features could not be programmed for some of the VLANs.

  Workaround: Remove the features and reapply. For PVLAN QoS, issuing a **no qos** and **qos** command will help. (CSCsc61449)

- On Cisco IOS Release 12.2(25)EWA4 and 12.2(25)EWA5, the system may crash during modification of a policy map attached to an interface with the **set ip {dscp|ip|precedence}** command.

Workaround: Remove the policy-map from the interface and re-configure a new policy-map without this option. (CSCsc97186)

- On a WS-C4948 running Cisco IOS Release 12.2(25)EWA3, you cannot re-set the interface MTU to the default.

  Workaround: Return the value of "Global Ethernet MTU" to the previous default value. (CSCsb81150)

- The following error messages may appear on a Catalyst 4900 series switch after reload, causing it to lose its VLAN configuration and preventing you from recreating them:

  This is observed on a switch whose VTP is in transparent mode, Version 2, after some non-default settings for VLANs 1003 and 1005 (token ring) were learned when the switch was in server mode.

  ```
  %SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error 14 from vtp
  function vtp_download_info: Bad parent VLAN ID-Traceback=...
  ```

  Workarounds:

  - Return to VTP version 1.
  - Use a 'ring' value in the range for 1 - 1005 for all Token Ring VLANs (CSCsc69560)

- When you configure “logging host X.X.X.X vrf,” on a WS-X4515 chassis that is running Cisco IOS Release 12.2(25)EWA5 or 12.2(25)SG, the chassis does not accept the command line to delete this configuration.

  Workaround: Issue the **erase start** command. (CSCek33573).

- If a physical interface is configured in shutdown mode, then configured with the same configuration including "switchport nonegotiate,” when it is later enabled by the **no shutdown** command, it can not join the bundle and the following error message displays:

  ```
  %EC-5-CANNOT_BUNDLE2: Gi3/16 is not compatible with Po1and will be suspended (trunk
  mode of Gi3/16 is dynamic, Po1 is trunk)
  ```

  The following configuration sequence will prevent interface g3/16 from joining the bundle:

  ```
  int g3/16
  shut
  switchport mode trunk
  switchport nonegotiate
  channel-group 1 mode on

  int po1
  switchport trunk enacp dot1q
  switchport mode trunk
  switchport nonegotiate

  int g3/16
   no shut
  ```

  Workaround: Do NOT configure the channel-port with the same configuration while all physical ports are still in shutdown mode. Instead, issue the **unshutdown** command on the physical ports to carry over the first unshutdown to the channel port. (CSCsd11234)

- When you set up a topology wherein a Catalyst 6000 series switch is connected by multiple links to Port 2, 15-16, 21-47 of a Catalyst 4948 series switch, after 1 minute, the blocking port of Catalyst 4948 starts flapping the STP port status.

  Workaround: Shutdown 2 ports to reduce the number of VLAN instances. (CSCsc29392)

- On a Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA2, dhcp snooping does not work on a PVLAN trunk.

Workaround: None (CSCej06004).

- The first multicast packet is dropped.

  Workaround: None (CSCsc51906).

- The BOOT variable is not cleared with the **no boot system** command.

  Workaround: Check the variable with the **show bootvar** command before issuing the **write memory** command. (CSCeg74620).

- If an interface is set to "not autonegotiate" from SNMP, and an snmp get is done to query the state of the interface, the correct state is returned. However, if the interface is set to "not autonegotiate" from the CLI, then an snmp get will show that it is still in autonegotiate mode, even though it isn't.

  Workaround: If the autonegotiate state is set by SNMP through the ifMauAutoNegAdminStatus value, it is reported by SNMP and CLI correctly. (CSCsc21274).

- When copying files to and from the switch, using ftp, the operation fails for files larger than 18528 bytes when the ftp server is on a remote network.

  A sample operation is:

  ```
  switch# copy running-conf ftp://user:password@n.n.n.n//users/xxx/switch-confg
  ```

  The error is:

  ```
  00:02:06: FTP: 550 /users/xxx/switch-confg: Broken pipe.
  ```

  Workaround: Either use a local ftp server on the same network or use tftp or rcp. (CSCsc48710).

- You might be the continuous error messages like:

  ```
  Dec 19 10:53:36: %C4K_PKTPROCESSING-4-UNKNOWNBRIDGEORROUTE: (Suppressed 52 times)
  Unable to determine whether to route or bridge replicated software-processed pa cket
  with source address 00:04:AC:E4:BC:38 and destination address 00:00:0C:07:AC:23

  Dec 19 11:03:45: %C4K_PKTPROCESSING-4-UNKNOWNBRIDGEORROUTE: (Suppressed 48 times)
  Unable to determine whether to route or bridge replicated software-processed packet
  with source address 00:04:AC:E4:BC:38 and destination address 00:00:0C:07:AC:23

  Dec 19 11:13:52: %C4K_PKTPROCESSING-4-UNKNOWNBRIDGEORROUTE: (Suppressed 37 times)
  Unable to determine whether to route or bridge replicated software-processed pa cket
  with source address 00:04:AC:E4:BC:38 and destination address 00:00:0C:07:AC:23
  ```

  Workaround: None (CSCsc87365).

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

(CCSCsd34759)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  (CSCek26492)

- The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

  (CSCek37177)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

  (CSCsd40334)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

  (CSCsd58381)

Open Caveats in Cisco IOS Release 12.2(25)EWA5

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA5:

- A QoS policing fails if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- On a Supervisor Engine V10-GE, when there are lot of flows in the system, an error message is logged to SYSLOG indicating that the netflow hardware table is full. The error message is misleading; the message states "flow table full" instead of "flow collisions."

  Workaround: None. (CSCeh97868)

- Occasionally, when a Catalyst 4900 series switch is in VTP client mode and “switchport trunk prunning vlan none” is configured on the trunk port, the trunk interface fails to send VLAN joins to the VTP server. Some of the VLAN is pruned on the link to the VTP server even when those VLANs are used.

  Workaround: Instead of using the "none" option, provide a specific VLAN when enabling VTP pruning on the trunk interface. (CSCei42957)

- While configuring Smartport macros via HTTP interactively, a Catalyst 4900 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsc05612)

- When VRF Packet Leaking is configured on a Catalyst 4900 series switch with a Supervisor Engine IV, a packet loss of 50 per cent occurs when you ping a Catalyst 4900 series switch VRF interface IP address from a device in the global table.

  Packets forwarded by Catalyst 4900 series switch are not impacted.

  Workaround: None. (CSCej36831)

- After you initially boot a Catalyst 4900 series switch, if the input interface is in PIM dense mode, “s,g” multicast cast traffic is not forwarded to the intended destination even if that group is represented by a “*,g” on the system.

  Workaround: Issue the **clear ip mroute *** command multiple times. (CSCsb50317)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA5

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA5:

- On the WS-4948G (RJ45 and SFP ports), WS-4948G-10GE (RJ45 ports only), WS-X4506-GB-T (RJ45 ports only), and WS-X4013+TS (RJ45 ports only), one or more ports may exhibit complete loss of traffic in both the transmit and receive directions. The problem can be seen on a port when its link flaps (up/down) multiple times in a short period of time.

  This problem impacts all IOS releases starting from Cisco IOS Release 12.2(25)EWA2 or later, including 12.2(25)SG. Entering the **shut** and **no shut** commands will not recover from this problem.

Please verify the following problem conditions to confirm the occurrence of this problem:

- Issue the **show interface** *module/port* **status** command; it displays the Connected state
- Issue the **show platform hardware interface GigabitEthernet** *module/port* **all**; it indicates that the MAC state is "Down" and that the rxInReset flag is set to "True"

Workaround: Reload the switch. (CSCsc10017)

- A WS-4948G, WS-4948G-10GE, WS-X4506-GB-T, and WS-X4013+TS might display the following message while running the Cisco IOS Release 12.2(20)EWA and later:

```
%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE: Blocked transmit queue HwTxQId1 on Switch Phyport
18,count=342141
```

Ports with a duplex mis-match and the switch port operating in half duplex will exhibit this problem and no traffic will flow through those ports.

Such a mis-match can occur when the switch port is configured for auto-negotiation but the far-end device is operating in forced mode. This mis-match can also occur when both ends of the link are operating in forced mode with the same speed but different duplex settings.

Workarounds:

- Issue shut /no shut to recover the port. (Prior to Cisco IOS Release 12.2(25)EWA2, a reload may be required.)
- Repair the duplex mis-match. Ensure that both the switch and the far-end device are both auto-negotiating or forced to operate at same speed and duplex. (CSCsb62330)

- A Catalyst 4900 series switch does not forward an 802.1X request with NULL credentials.

  Workaround: None. (CSCej03858)

- A port enabled for Loop Guard that participates in spanning tree (and is in BLK state) goes into a loop inconsistent state when it stops receiving BPDUs from its neighbor. When the neighbor resumes sending BPDUs (instead of STP BPDUs), STP ordinarily recovers from this state. For this caveat, STP does not recover and the port remains stuck.

  Workarounds:

  - Enter the **shut** and **no shut** commands on the port.
  - Disable Loop Guard on the port and then re-enable it. (CSCsc04047)

- A Catalyst 4900 series switch with Supervisor Engine IV running Cisco IOS Release 12.2(25)EWA3 will send an ARP packet (from an STP blocking port) that can cause a broadcast storm when you either reload a Catalyst 4900 series switch with a blocking port or enter **shut** and **no shut** commands on any port of the switch.

  Workaround: None. (CSCsb84685)

- If UDLD is enabled on a trunk port with native VLAN tagging enabled, the UDLD protocol packets are sent out untagged. This may cause UDLD interoperability issues with other Cisco switches that expect to always see tagged packets on trunk ports.

  Workaround: None. (CSCsb34771)

Open Caveats in Cisco IOS Release 12.2(25)EWA4

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA4:

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature shows only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands are accepted, even after you enter the **macro apply** command. (CSCsa44632)

- QoS policing fails if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- After you initially boot a Catalyst 4900 series switch, if the input interface is in PIM dense mode, “s,g” multicast cast traffic is not forwarded to the intended destination even if that group is represented by a “*,g” on the system.

  Workaround: Issue the **clear ip mroute *** command multiple times. (CSCsb50317)

- On a Supervisor Engine V10-GE, when there are lot of flows in the system, an error message is logged to SYSLOG indicating that the netflow hardware table is full. The error message is misleading; the message states "flow table full" instead of "flow collisions."

  Workaround: None. (CSCeh97868)

- Occasionally, when a Catalyst 4900 series switch is in VTP client mode and “switchport trunk prunning vlan none” is configured on the trunk port, the trunk interface fails to send VLAN joins to the VTP server. Some of the VLAN is pruned on the link to the VTP server even when those VLANs are used.

  Workaround: Instead of using the "none" option, you must provide a specific VLAN when enabling VTP pruning on the trunk interface. (CSCei42957)

- If UDLD is enabled on a trunk port with native VLAN tagging enabled, the UDLD protocol packets are sent out untagged. This may cause UDLD interoperability issues with other Cisco switches that expect to always see tagged packets on trunk ports.

  Workaround: None. (CSCsb34771)

- While configuring Smartport macros via HTTP interactively, a Catalyst 4900 series switch might restart unexpectedly.

  Workaround: Provide the entire command sequence in the browser "command" area as if you were entering the commands through the CLI. (CSCei76082)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA4

This section lists the resolved caveats in Cisco IOS Release 12.2(25)EWA4:

- Issuing the **no ip flow ingress** command does not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- Modifying a policer may not work if you configure more than 800 policers.

Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- The **dot1x default** command does not restore the defaults for the **dot1x max-reauth-req** and **dot1x timeout reauth server** commands.

  Workaround: Restore these default values manually. (CSCeh97513)

- After vty is set to "never," it cannot be released with the **clear line XX** command.

  Workaround: Reload the system. (CSCei26830)

Note Always exit the global configuration mode *before* a switchover.

- After changing the SNMP engine ID on a Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA, none of the existing community strings work. You must re-establish the relationship between any community strings and the new engine ID.

  Upon issuing the **snmp mib community-map** command, you will observe additional SNMP configuration entries that reflect the mismatched SNMP engine ID.

  Workaround: Remove the community-map with the **no snmp mib community-map** command. (CSCei29841)

- With IP multicast routing and IGMP snooping enabled, a Catalyst 4900 series switch does not send ARP requests to a partner switch if the trunk port on the Catalyst 4900 switch is the only interface carrying private VLANs.

  Workaround: Configure any other port on the Catalyst 4900 switch (not necessarily one connected to the partner switch) as a regular trunk interface. Ensure that the interface is "link up" and carries both primary and isolated VLANs. (CSCsb06924)

- If an 802.1X supplicant logs off, the AAA Accounting Stop record displays "port-error" as the Acct-Terminate-Cause[49] reason instead of "user-req."

  Workaround: None.(CSCsb36480)

- A Catalyst 4900 series switch running the Cisco IOS Release 12.2(25)EWA2 does not send LinkUp traps (IF-MIB).

  Workaround: Issue the **snmp trap link-status permit duplicates** command on the interfaces. (CSCsb38308)

- Executing the **show** command in trustpoint-ca configuration mode might cause the switch to fail by corrupting the stack.

  Workaround: Do not issue the **show** command in trust-ca configuration mode. (CSCsb42958)

- When 802.1X accounting is enabled, the Framed-IP-Address[8] attribute is not included in accounting messages generated on ports with IP DHCP snooping trust enabled.

  Workaround: None. (CSCsb46019)

- If storm control is configured and you manually toggle the link (up/down), the ARP table no longer updates its database.

  Workaround: Allow storm control to disable and enable the interface. (CSCsb49409)

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml. (CSCei61732)

Open Caveats in Cisco IOS Release 12.2(25)EWA3

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA3:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
Switch# show policy-map int
 FastEthernet6/2

  Service-policy output: p4

    Class-map: ipc2 (match-all)
      0 packets<---------- It shouldn't stay at '0'.
      Match: access-group name ipacl_2
      police: Per-interface
        Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru
```

```
Class-map: class-default (match-any)
  410 packets
  Match: any
    410 packets
```

Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA3

This section lists the resolved caveats in Release 12.2(25)EWA3:

- Through normal software maintenance processes, Cisco is removing deprecated functionality from the OS boot routine. These changes have no impact on system operation or feature availability. (CSCei76358)

Open Caveats in Cisco IOS Release 12.2(25)EWA2

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA2:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
Switch# show policy-map int
 FastEthernet6/2

  Service-policy output: p4

    Class-map: ipc2 (match-all)
      0 packets<---------- It shouldn't stay at '0'.
      Match: access-group name ipacl_2
      police: Per-interface
        Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


    Class-map: class-default (match-any)
      410 packets
      Match: any
        410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA2

This section lists the resolved caveats in Release 12.2(25)EWA2:

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

  ```
  Switch(config)#snmp-ser enable traps port-se trap-rate 1
  Switch(config)#snmp-ser enable traps port-se trap-rate 2
  ```

- If you configure a SPAN session and then apply a SPAN ACL filter to the session, the packets that should be dropped according to the ACL definition are still sent out the SPAN destination port.

  For example, the intent of the following command sequence is to drop packets with source or destination IP address 20.4.1.2 on the SPAN destination port Gigabit Ethernet 6/5:

  ```
  Switch(config)# access-list 1 deny 20.4.1.2
  Switch(config)# monitor session 1 source interface gi6/5
  Switch(config)# monitor session 1 destination interface gi6/7
  Switch(config)# monitor session 1 filter ip access-group 1
  ```

  However, if this is the first time you are applying the ACL filter to the SPAN session, the packets with IP address 20.4.1.2 are still copied to the SPAN destination port.

  If this sample configuration is contained in the startup-config, then the ACL filter would work properly after the Catalyst 4900 series switch boots.

  This caveat only impacts Cisco IOS Release 12.2(25)EWA.

  Workaround: Remove the ACL filter and then re-apply it using the following command sequence:

  ```
  Switch(config)# no monitor session 1 filter ip access-group 1
  Switch(config)# monitor session 1 filter ip access-group 1
  ```

  (CSCsa64231)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- When you use the **vlan** command in interface range configuration mode to configure a range of VLANs on Layer 3 ports, the VLANs might not be created, as in the following example. Additional VLANs will not be created on the Catalyst 4900 series switch until the switch has been reloaded.

  ```
  Switch(config)# int range gi3/3 - 28
  Switch(config-if-range)# sw
  Switch(config-if-range)# no sw
  Switch(config-if-range)# vlan 1000-4094
  % Command failed on interface GigabitEthernet3/4. Aborting
  Switch(config)#
  ```

  Workaround: Create the VLANs in global or interface command mode. CSCsa54831)

- Under load conditions, the CPU utilization reported on a Catalyst 4900 series switch running Cisco IOS Release 12.2(25)EWA2 is approximately 5 per cent higher than that reported on previous releases of IOS.

Workaround: In previous releases of Cisco IOS, CPU utilization was computed incorrectly. This defect has been fixed in Cisco IOS Release 12.2(25)EWA2 resulting in slightly higher CPU utilization being reported under similar load conditions as compared to previous releases. (CSCsb19391)

This is not a problem and a workaround is unnecessary.

- A QoS service-policy cannot be attached to a port or VLAN if routing is not configured on the system.

  Workaround: Enable IP routing on the system, but do not configure any SVIs and or physical routed ports. The routing operation is performed only when a SVI and or physical routed port is configured with a valid IP address. (CSCsa54215)

- When you configure numerous per-port per-VLAN QoS (like 800 input policers), and then modify them, per-port per-VLAN QoS will stop working.

  Workaround: Disable and or re-enable QoS. (CSCsa66422)

- Occasionally, when IPX ACL is configured with a tunnel interface to carry IPX traffic, the Catalyst 4900 series switch reloads once you delete the interface.

  This caveat does not occur in earlier releases.

  Workaround: None. (CSCsa68817)

Open Caveats in Cisco IOS Release 12.2(25)EWA1

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA1:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

```
Switch(config)#snmp-ser enable traps port-se trap-rate 1
Switch(config)#snmp-ser enable traps port-se trap-rate 2
```

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
Switch# show policy-map int
 FastEthernet6/2

  Service-policy output: p4

    Class-map: ipc2 (match-all)
      0 packets<---------- It shouldn't stay at '0'.
      Match: access-group name ipacl_2
      police: Per-interface
        Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


    Class-map: class-default (match-any)
      410 packets
      Match: any
        410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When a switchport configured with port security is converted from an access to a promiscuous port, the port security configuration is lost. The **show interface** command will show that port security is no longer configured.

  Workaround: After converting a switchport with port security to a promiscuous port, apply the port security interface command again. (CSCeg41424)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- If you configure a SPAN session and then apply a SPAN ACL filter to the session, the packets that should be dropped according to the ACL definition are still sent out the SPAN destination port.

For example, the intent of the following command sequence is to drop packets with source or destination IP address 20.4.1.2 on the SPAN destination port Gigabit Ethernet 6/5:

```
Switch(config)# access-list 1 deny 20.4.1.2
Switch(config)# monitor session 1 source interface gi6/5
Switch(config)# monitor session 1 destination interface gi6/7
Switch(config)# monitor session 1 filter ip access-group 1
```

However, if this is the first time you are applying the ACL filter to the SPAN session, the packets with IP address 20.4.1.2 are still copied to the SPAN destination port.

If this sample configuration is contained in the startup-config, then the ACL filter would work properly after the Catalyst 4900 series switch boots.

This caveat only impacts Cisco IOS Release 12.2(25)EWA.

Workaround: Remove the ACL filter and then re-apply it using the following command sequence:

```
Switch(config)# no monitor session 1 filter ip access-group 1
Switch(config)# monitor session 1 filter ip access-group 1
```

(CSCsa64231)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- When you use the **vlan** command in interface range configuration mode to configure a range of VLANs on Layer 3 ports, the VLANs might not be created, as in the following example. Additional VLANs will not be created on the Catalyst 4900 series switch until the switch has been reloaded.

  ```
  Switch(config)# int range gi3/3 - 28
  Switch(config-if-range)# sw
  Switch(config-if-range)# no sw
  Switch(config-if-range)# vlan 1000-4094
  % Command failed on interface GigabitEthernet3/4. Aborting
  Switch(config)#
  ```

  Workaround: Create the VLANs in global or interface command mode. CSCsa54831)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA1

This section lists the resolved caveats in Release 12.2(25)EWA1:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

(CSCsa81379)

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml. (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(25)EWA

This section lists the open caveats in Cisco IOS Release 12.2(25)EWA:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

```
Switch(config)#snmp-ser enable traps port-se trap-rate 1
Switch(config)#snmp-ser enable traps port-se trap-rate 2
```

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
Switch# show policy-map int
 FastEthernet6/2

  Service-policy output: p4

    Class-map: ipc2 (match-all)
      0 packets<---------- It shouldn't stay at '0'.
      Match: access-group name ipacl_2
      police: Per-interface
        Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


    Class-map: class-default (match-any)
      410 packets
      Match: any
        410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When a switchport configured with port security is converted from an access to a promiscuous port, the port security configuration is lost. The **show interface** command will show that port security is no longer configured.

  Workaround: After converting a switchport with port security to a promiscuous port, apply the port security interface command again. (CSCeg41424)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- If you configure a SPAN session and then apply a SPAN ACL filter to the session, the packets that should be dropped according to the ACL definition are still sent out the SPAN destination port.

  For example, the intent of the following command sequence is to drop packets with source or destination IP address 20.4.1.2 on the SPAN destination port Gigabit Ethernet 6/5:

```
Switch(config)# access-list 1 deny 20.4.1.2
Switch(config)# monitor session 1 source interface gi6/5
Switch(config)# monitor session 1 destination interface gi6/7
Switch(config)# monitor session 1 filter ip access-group 1
```

  However, if this is the first time you are applying the ACL filter to the SPAN session, the packets with IP address 20.4.1.2 are still copied to the SPAN destination port.

  If this sample configuration is contained in the startup-config, then the ACL filter would work properly after the Catalyst 4900 series switch boots.

  This caveat only impacts Cisco IOS Release 12.2(25)EWA.

  Workaround: Remove the ACL filter and then re-apply it using the following command sequence:

```
Switch(config)# no monitor session 1 filter ip access-group 1
Switch(config)# monitor session 1 filter ip access-group 1
```

  (CSCsa64231)

- Issuing the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command.

  (CSCsa67042)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers. (CSCsa57218)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- When you use the **vlan** command in interface range configuration mode to configure a range of VLANs on Layer 3 ports, the VLANs might not be created, as in the following example. Additional VLANs will not be created on the Catalyst 4900 series switch until the switch has been reloaded.

```
Switch(config)# int range gi3/3 - 28
Switch(config-if-range)# sw
Switch(config-if-range)# no sw
Switch(config-if-range)# vlan 1000-4094
% Command failed on interface GigabitEthernet3/4. Aborting
Switch(config)#
```

  Workaround: Create the VLANs in global or interface command mode. CSCsa54831)

Resolved Caveats in Cisco IOS Release 12.2(25)EWA

This section lists the resolved caveats in Release 12.2(25)EWA:

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When the access VLAN of an access port is converted into an RSPAN VLAN, the **show interface** and **show interface inactive** commands indicate that the interface is up and connected. This problem is strictly cosmetic; the interface is no longer forwarding traffic.

  Workaround: None. (CSCsa44090)

- When a Catalyst 4900 series switch exhausts the packet buffers and can no longer receive packets, the Rx-No_pkt_Buff field in the output of the **show platform interface all** command may not get updated.

  Workaround: None. (CSCef72691)

- Per-flow Border Gateway Protocol (BGP) AS information is not collected. As a result, BGP AS information will not be available in any of the aggregation caches.

  Workaround: None. (CSCin85662)

- Multicast over Generic Routing Encapsulation (GRE) does not work.

  Workaround: None (CSCin85525)

Open Caveats in Cisco IOS Release 12.2(25)EW

This section lists the open caveats in Cisco IOS Release 12.2(25)EW.

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- When the access VLAN of an access port is converted into an RSPAN VLAN, the **show interface** and **show interface inactive** commands indicate that the interface is up and connected. This problem is strictly cosmetic; the interface is no longer forwarding traffic.

  Workaround: None. (CSCsa44090)

- When a Catalyst 4900 series switch exhausts the packet buffers and can no longer receive packets, the Rx-No_pkt_Buff field in the output of the **show platform interface all** command may not get updated.

  Workaround: None. (CSCef72691)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- Per-flow Border Gateway Protocol (BGP) AS information is not collected. As a result, BGP AS information will not be available in any of the aggregation caches.

  Workaround: None. (CSCin85662)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
Switch# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- Multicast over Generic Routing Encapsulation (GRE) does not work.

  Workaround: None (CSCin85525)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- If the switch receives an unlearned source MAC address after a security violation, memory is consumed in creating a security violation-related SNMP trap for each source MAC address. If the switch receives several unlearned source MAC addresses at a very high rate, considerable memory is consumed to ensure that the SNMP traps are generated and sent out correctly.

  Workaround: Configure the trap-rate to limit very small number of traps every second. The following configuration sets a trap-rate of 1/2 trap per second (CSCeg41478):

```
Switch(config)#snmp-ser enable traps port-se trap-rate 1
Switch(config)#snmp-ser enable traps port-se trap-rate 2
```

- Under certain rare scenarios, the packet match counter in **show policy-map interface fa6/1** does not show the packets being matched, as in the following configuration:

```
Switch# show policy-map int
 FastEthernet6/2

  Service-policy output: p4

    Class-map: ipc2 (match-all)
      0 packets<---------- It shouldn't stay at '0'.
      Match: access-group name ipacl_2
      police: Per-interface
        Conform: 22937970 bytes Exceed: 977688712 bytes <--- traffic going thru


    Class-map: class-default (match-any)
      410 packets
      Match: any
        410 packets
```

  Workaround: Either enter a shutdown/no shutdown on the port or detach and reapply the service policy. (CSCef30883)

- When a switchport configured with port security is converted from an access to a promiscuous port, the port security configuration is lost. The **show interface** command will show that port security is no longer configured.

  Workaround: After converting a switchport with port security to a promiscuous port, apply the port security interface command again. (CSCeg41424)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

Resolved Caveats in Cisco IOS Release 12.2(25)EW

This section lists the resolved caveats in Release 12.2(25)EW:

- Under conditions where switch communication with the RADIUS server is broken or delayed, 802.1X may either cause the switch to crash or generate memory corruption tracebacks. This issue impacts Release 12.2(20)EWA.

  Workaround: None. (CSCef46146)

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml. (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(20)EWA4

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA4:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA4

This section lists the resolved caveats in Release 12.2(20)EWA4:

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  (CSCek26492)

- Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  (CSCec71950)

Open Caveats in Cisco IOS Release 12.2(20)EWA3

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA3:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

Workaround: Disable idle timeouts. (CSCec30214)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA3

This section lists the resolved caveats in Release 12.2(20)EWA3:

- Through normal software maintenance processes, Cisco is removing deprecated functionality from the OS boot routine. These changes have no impact on system operation or feature availability. (CSCei76358)

Open Caveats in Cisco IOS Release 12.2(20)EWA2

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA2:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA2

This section lists the resolved caveats in Release 12.2(20)EWA2:

- Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml. (CSCef68324)

Open Caveats in Cisco IOS Release 12.2(20)EWA1

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA1:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA1

This section lists the resolved caveats in Release 12.2(20)EWA1:

- NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

```
cnfFeatureAcceleration        1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable  1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot       1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot          1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable               1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry               1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType                1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot                1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive              1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches            1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges       1.3.6.1.4.1.9.9.99999.1.3.4.1.6
```

  (CSCsa81379)

Open Caveats in Cisco IOS Release 12.2(20)EWA

This section lists the open caveats in Cisco IOS Release 12.2(20)EWA.

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then reenable QoS with the **qos global** command. (CSCee52449)

- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

Resolved Caveats in Cisco IOS Release 12.2(20)EWA

This section lists the resolved caveats in Release 12.2(20)EWA:

- The DHCP snooping database agent has a maximum of 8192 entries. If the number of DHCP bindings learned by the system exceeds this number, the entries in the database agent will be cleared out, the entries in hardware will be retained, and switching will continue. However, upon reload, bindings and connectivity will be lost.

  Workaround: None. (CSCee34375)

- If IP source guard and QoS policies with large ACLs are configured on an interface, deleting the QoS policy will not clear the policers from the hardware.

  Workaround: Either remove the IP source guard configuration using the **no ip verify source vlan dhcp-snooping port-security** command and reconfigure using the **ip verify source vlan dhcp-snooping port-security** command or shut down the interface (after removing the policy) using the **shutdown** command, and reactivate it using the **no shutdown** command. (CSCee44402)

- When you use private VLANs on the Catalyst 4900 series switch, old ARP entries will not timeout of the ARP cache without manually clearing the ARP entry. This has no effect on production.

  Workaround: Issue the **clear arp** command on the supervisor engine. (CSCee73094)

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4900 family running IOS supervisor engines:

- Netbooting from the ROMMON, page 128
- Troubleshooting at the System Level, page 129
- Troubleshooting Modules, page 129
- Troubleshooting MIBs, page 129

Netbooting from the ROMMON

Netbooting using a boot loader image is not supported. Instead, use one of the following options to boot an image:

1. Boot from a CompactFlash card by entering the following command:

   ```
   rommon 1> boot slot0:<bootable_image>
   ```

2. Use ROMMON TFTP boot.

   The ROMMON TFTP boot is very similar to the BOOTLDR TFTP boot, except that:

   - the BOOTLDR variable should *not* be set
   - the TFTP server must be accessible from the Ethernet management port on the supervisor engine.

To boot from ROMMON, perform the following tasks while in ROMMON mode:

a. Ensure that the Ethernet management port is physically connected to the network.

b. Verify that bootloader environment is not set by entering the **unset bootldr** command.

c. Set IP address of the Ethernet management port on the supervisor engine by entering the following command: **set interface fa1** *ip_address*> <*ip_mask*

   For example, to set the supervisor engine Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0, enter the following command:

   ```
   rommon 2> set interface fa1 172.16.1.5 255.255.255.0
   ```

d. Set default gateway for the Ethernet management port on the supervisor engine by entering the following command: **set ip route default** *gateway_ip_address*. The default gateway should be directly connected to the supervisor engine Ethernet management port subnet.

e. Ping the TFTP server to ensure that there is connectivity to the server from the Ethernet management port on the supervisor engine by entering the following command: **ping** <*tftp_server_ip_address*>.

f. Once the ping is successful, boot the image from the TFTP server by entering the following command: **boot tftp://***tftp_server_ip_address*>**/**<*image_path_and_file_name*

   For example, to boot the image name **cat4500-is-mz** located on the TFTP server 172.16.1.8, enter the following command:

   ```
   rommon 3> boot tftp://172.16.1.8/tftpboot/cat4500-is-mz
   ```

Troubleshooting at the System Level

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- Ensure that you do not mix the serial and Ethernet cables. The Ethernet Management port is inoperative in all Cisco IOS releases (Cisco IOS Release 12.2(20)EWA through Cisco IOS Release 12.2(31)SGA). An Ethernet cable plugged into the Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for the Catalyst 4900 series switch:

- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, ensure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the port set to autonegotiate will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

Troubleshooting MIBs

For general information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml). For information on the specific MIBs supported by the Catalyst 4900 series switches, refer to the Catalyst 4000 MIB Support List located at ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html.

Related Documentation

These sections describe the documentation available for the Cisco IOS software for the Catalyst 4900 series switch. These publications consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other publications. Documentation is available electronically or in printed form.

Use these release notes with the publications listed in the following sections:

- Release-Specific Publications, page 130
- Platform-Specific Publications, page 130
- Cisco IOS Software Documentation Set, page 130

Release-Specific Publications

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html

Platform-Specific Publications

These publications are available for the Catalyst 4900 series switch running the Cisco IOS software at the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html

- *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 4500 Series Switch Cisco IOS Command Reference*
- *Catalyst 4500 Series Switch Cisco IOS System Message Guide*

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting publications.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. You can use each configuration guide in conjunction with its corresponding command reference. On Cisco.com, two master hot-linked publications provide information for the Cisco IOS software documentation set.

Release 12.2 Documentation Set

The following table describes the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and orderable in printed form.

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
• *Cisco IOS IP and IP Routing Configuration Guide* • *Cisco IOS IP and IP Routing Command Reference*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS Multiservice Applications Configuration Guide* • *Cisco IOS Multiservice Applications Command Reference*	Multiservice Applications Overview Voice Video Broadband
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping signaling Link Efficiency Mechanisms Quality of Service Solutions
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features

Books	Major Topics
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching MPLS Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • Release Notes (release note and caveat documentation for 12.2-based releases and various platforms) • *Cisco IOS Debug Command Reference* • *Cisco IOS Dial Services Quick Configuration Guide*	

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)

Release Notes for the Catalyst 4900 Series Switch, Cisco IOS Release 12.2(40)SG
Copyright © 1999–2008, Cisco Systems, Inc. All rights reserved.